CELTIC Project Number:	**C2012/2-5**
Project Title:	SDN Concept in Generalized Mobile Network Architectures – SIGMONA
Confidentiality:	PU / RE / CO[1]

Document Identifier:	D3.1
Document Title:	**State-of-the-art and challenges of traffic, resource and mobility management in software-defined mobile networks**
Authors:	Zoltán Faigl
Participants:	See authors section
Work Package:	WP3
Version:	Final version
Date of last changes:	27.02.2015
File Name:	D3.1.pdf

Abstract: This document surveys the state-of-the-art and collects specific research challenges of resource, traffic and mobility management in software-defined, vitrualized mobile networks

Keywords: software-defined mobile networks, resource management, traffic management, mobility management, state-of-the-art, challenges software-defined networks, network function virtualization

Disclaimer:

Document History:	
25.11.2014	1st release
25.02.2015	Final version

[1] Dissemination level:
PU = Public
RE = Distribution to a group specified by the consortium
CO = Confidential, only allowed for members of the consortium

Table of Contents

Authors

Partner	Name	Phone / Fax / e-mail
Budapest University of Techn. and Econ., Mobile Innovation Centre		
	Zoltán Faigl	
		Phone: +36 1 463 2500
		e-mail: zfaigl@mik.bme.hu
	László Bokor	
		Phone: +36 1 463 2048
		e-mail: bokorl@hit.bme.hu
University of Oulu, Center of Wireless Communications		
	Suneth Namal	
		Phone:
		e-mail: gkarunar@ee.oulu.fi
Technical University of Chemnitz		
	Thomas Bauschert	
		Phone:
		e-mail: thomas.bauschert@etit.tu-chemnitz.de
	Marcus Eckert	
		Phone:
		e-mail: marcus.eckert@etit.tu-chemnitz.de
NEXTEL		
	Oscar López	
		Phone:+34 94 40355 55
		e-mail: olopez@nextel.es
	Mikel Uriarte Itzazelaia	
		Phone: :+34 94 40355 55
		e-mail: muriarte@nextel.es
ENEO		
	Jaime Nebrera	
		Phone:
		e-mail: jnebrera@eneotecnologia.com
Innovalia Association		
	Daniel Alcaraz Real-Arce	
		Phone:
		e-mail: dalcaraz@innovalia.org
Turk Telekom		
	Aydın Ulaş	
		Phone: +90 212 707 52 19
		e-mail: aydin.ulas@argela.com.tr

Ericsson Turkey		
	Hasan Anıl Akyıldız	
		Phone:
		e-mail: hasan.anil.akyildiz@ericsson.com
	Ece Saygun	
		Phone:
		e-mail: ece.saygun@ericsson.com

BULL SAS		
	Gérard Jacquet	
		Phone:
		e-mail: gerardjacquet@bull.net
	Olivier Jard	
		Phone:
		e-mail: olivier.jard@bull.net

CEA LIST		
	Michael BOC	
		Phone: +33 (0) 1 69 08 39 76
		e-mail: Michael.Boc@cea.fr
	Mohamed LABRAOUI	
		Phone: +33 (0)1 69 08 07 28
		e-mail: Mohamed.Labraoui@cea.fr

Executive Summary

This document surveys the state-of-the-art and standardization in software-defined, vitrualized mobile networks, and collects the use cases, basic assumptions and research challenges related to resource, traffic and mobility management in the Celtic-Plus SIGMONA project.

The main resource, traffic and mobility management use cases are the following:

Resource management:

- Resource availability awareness in SDMNs
- Optimized video delivery

Macroscopic-level traffic management :

- Joint traffic and cloud resource management for service chaining in SDMNs
- Coordinated traffic and resource management and efficient routing in SDMNs
- Application-level traffic optimization in SDMNs

Microscopic-level traffic management :

- DiffServ QoS in SDN-based transport and policy control in SDMNs
- Quality of Service/Experience Enforcement

Mobility management

- Extension of legacy solutions for mobility management in SDMNs
- SDN based extensions to LTE/EPC mobility management
- Enabling secure network mobility with OpenFlow

The proposed technology solutions and description of introduced functions and interfaces of our use cases is expected to be specified in forthcoming deliverables.

List of abbreviations

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ADMM	Alternating Direction Method of Multipliers
AE	Authorization Entity
AF	Application Function (in PCC architecture), Assured Forwarding (In DiffServ concept)
ALTO	Application-Layer Traffic Optimization
AMBR	Aggregate Maximum Bit Rate
ANDSF	Access Network Discovery and Selection Function
AR	Access Router
ARP	Allocation and Retention Priority
API	Application Programming Interface
APN	Access Point Name
AS	Autonumous Service
BA	Behavior Aggregate
BBERF	Bearer Binding and Event Reporting Function
CAPEX	Capital Expenditure
CBR	Constant Bit Rate
CBQ	Class-based Queueing
CDN	Content Distribution Network
CN	Correspondent Node
DHCP	Dynamic Host Configuration Protocol
DHT	Distributed Hast Table
DL	Downlink
DiffServ / DS	Differentiated Services
DMM	Distributed Mobility Management
DSCP	Differentiated Services Code Point
E-E	End-to-End
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved-UMTS Terrestrial Radio Access Network
FMIP	Fast Handoffs for Mobile IPv6
FPTAS	Fully Polynomial Time Approximation Schemes
FTP	File Transfer Protocol
GBR	Guaranteed Bitrate
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node (GGSN)
GPRS	General Packet Radio Service
GTP	GPRS Tunneling Protocol
HA	Home Agent (MIP context), Host association (HIP context)
HAWAII	Handoff-Aware Wireless Access Internet infrastructure
HFSC	Hierarchical Fair-Service Queue
HIP	Host Identity Protocol
HMIP	Hierarchical Mobile IP
HRPD	High Rate Packet data
HTB	Hierarhical Token Bucket
IaaS	Infrastructure-as-a-Service
IETF	Internet Engineering Task Force

IKEv2	Internet Key Exchange version 2
IntServ	Integrated Services
IMS	IP Multimedia Subsystem
IPv4 / IPv6	Internet Protocol version 4 / version 6
ISG	Industry Specification Group
ISIS	Intermediate System to Intermediate System
ISP	Internet Service Provider
LAN	Local Area Network
LIPA	Local IP Traffic Offload
LLDP	Link-Layer Discovery Protocol
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MIP	Mobile IP
MBR	Maximum Bitrate
MCoA	Multiple Care-of Addresses
MPLS	Multiprotocol Label Switching
MAG	Mobility Anchor Gateway
MM	Mobility Management
MN	Mobile Node
MNN	Mobile Network Node
MNO	Mobile Network Operator
MR	Mobile Router
NE	Network Element
NEMO	Network Mobility
NFV	Network Function Virtualization
NOS	Network Operating System
OF	OpenFlow
ONF	Open Network Foundation
OPEX	Operational Expenditure
OSPF	Open Shortest Path First
P2P	Peert-to-Peer
PaaS	Platform-as-a-Service
PCC	Policy Control and Charging
PCEF	Policy Control Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDP	Packet Data Protocol
P-GW	PDN Gateway
PHB	Per Hop Behaviour
PID	Provider-defined Identifier
PMIP	Proxy Mobile IP
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of service
PID	Provider-defined Identifer
RAN	Radio Access Network
RSVP	Resource Reservation Protocol
RNC	Radio Network controller
RTT	Round-Trip Time
SCTP	Stream Control Transmission Protocol
SDF	Service data Flow
SDN	Software-Defined Network

SDMN	Software-Defined Mobile Network
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SIP	Session Initiation Protocol
SIPTO	Selective IP Traffic Offload
SLA	Service-Level Agreement
SPR	Subscription Profile Repository
TCA	Traffic Conditioning Agreement
TE	Traffic Engineering
TEID	Tunnel Endpoint Identifier
TFT	Traffic Flow Template
TM	Traffic Management
TOR	Top of Rack switch
TTL	Time-to-live
UE	Useer Equipment
UL	Uplink
UTRAN	UMTS Terrestrial Radio Access Network
VLAN	Virtual LAN
VMNO	Virtual Mobile Network Operator
VM	Virtual Machine
VNP	Virtual Network Provider
VirtMobOpt	Virtualization-based Optimisation of Mobile Networks
VTN	Virtual Tenant Network
WFQ	Weighted Fair Queueing
WRR	Weighted Round-Robin

1. Introduction

Due to the evolution of mobile transmission technologies since GSM to 3G, 4G, in these days high-speed data services are dominating in mobile networks both in uplink and downlink. The traditional voice calls are only a small proportion of traffic demands.Users expect high-speed services both in downlink and in uplink, independently of their location, and the available access technologies. Content providers, content distribution networks also require smart resource and traffic management in order to minimize their transport costs and better utilize network, resources.

Taking into accout data services features, the usage patterns, the user, network mobility patterns, and the utilization of network resources are continuously changing in time and location. As the volume of traffic demands increases, the amplitude of their variations grows as well. Existing network, resource, traffic and mobility management mechanisms are too inflexible to adapt to these demands.

Therefore, the SIGMONA project will investigate in three topics software-defined networking (SDN), network functions virtualization (NFV) and cloud-service paradigms, which will enable less human intervention in network operation, and better utilization of resources, hence less CAPEX and OPEX, and additionally more flexibility to fulfil new demands. These demands will imply new business models for radio access network, transport network and/or core network sharing, e.g., by virtualization of certain network functions of the mobile network, or by selling whole slices of the mobile network by virtual network providers (VNP) to virtual mobile network operators (VMNO).

The objective of this deliverble is to survey existing state-of-the-art solutions and standardization for novel resource management (RM), traffic management (TM) and mobility management (MM) techniques in the above-mentioned environment related to mobile networks, which make use of the paradigms of SDN, NFV,actually increasingly and wider used for large content and cloud-service providers and Content Delivery Networks (CDNs). An important aspect is that the recommended solutions must be suitable for interworking with the untouched network components of the mobile network.

Integration and optimization of RM, TM and MM within partly SDN-, NFV- and cloud-service based mobile network architectures need that we analyse possible use cases, scenarios, and basic assumptions of these areas in Software-Defined Mobile Networks (SDMNs).

In Section 2, we survey the related work found in state-of-the-art. Section 3 summarizes the main use cases of Open Network Foundation (ONF) and ETSI NFV Industry Specification Group related to RM, TM and MM. Section 4 collects the main research challenges related to our use cases. The relations between the research topics and the basic assumptions of the SIGMONA project are also described. Section 5 describes our use cases and scenarios; finally, Section 6 concludes this deliverable. Appendix A summarizes the commonly used protocols for resource management, while Appendix B describes the main terms and mechanisms of QoS control in LTE/EPC.

2. State-of-the-art

This chapter presents the state-of-the-art related to resource, traffic and mobility management in mobile networks.

- Section 2.1 defines the objectives of resource management, and summarizes the related problem areas in regards of resource awareness, slice embedding, cloud resource management, video streaming.
- Section 2.2 presents the objectives of traffic management, and the related problem areas in SDMNs, i.e., QoS-aware routing, service chaining, QoS provisioning.
- Section 2.3 describes the problem areas of mobility management in SDMNs, state-of-the-art mobility management, introduction of virtualization technologies, existing proposals.

2.1 Resource management

This section discusses the state-of-the-art of resource management related to the topic of software-defined mobile networks.

2.1.1 Definition of resource management

The network is always a shared resource, either outside the server chassis - by using central cables, switches, or routers - or inside the chassis - by sharing physical ports, network stacks, or just the CPUs that are handling the traffic by doing checksumming or handling the network adapter interrupts.

To meet the different service level agreements (SLAs) of the network consumers, network resource management is needed. The requirements can be based on available network bandwidth, the network latency, or the network data loss rate. While network latency and data loss rate are typically based on the network technology that is used and the OS, or in the case of virtualized environments the hypervisor-specific implementation, the available bandwidth can be controlled by resource management.

2.1.2 Why Resource Management is important?

Resource management limits access to shared resources, but it also monitors resource consumption and collects accounting information.

The management of resources is important, because many consumers request resources. Consolidating different workloads on one system often entails combining workloads that have different service level agreements and different needs for throughput, response time, and availability.

But resources are always limited, and they are shared among many environments on one IT system; therefore, it is important to restrict access to specific shared resources, isolate resources from being used by certain workloads, or at least limit shared resource consumption of workloads. By doing that, we can guarantee a service level for each environment or influence its performance.

Without resource management, all workloads would be handled equally, based on their resource requests. The result could be that one machine consumes so much memory during runtime that others on the same system get blocked and important memory requests can no longer be served, due to no available memory. Another example of the importance of resource management is the ability to determine how many resources should be shown to or seen by the rest of the elements of the network.

An efficient resource management should cover at least the following aspects:

- Prevent entities from consuming unlimited resources
- Be able to change a priority, based on external events
- Balance resource guarantees against the goal of maximizing system utilization

2.1.3 Resource Management on Virtualized Networks

Virtual networks are aiming at better utilization of the underlying infrastructure in terms of reusing a single physical or logical resource for multiple other network instances, or to aggregate multiple of these resources, in order to obtain more functionality, such as providing a pool of resources that can be utilized on demand. These resources can be network components such as routers, switches, hosts, or virtual machines. As state, these virtual machines can execute virtual routers or virtual service elements, but can also execute network services such as name mapping systems. In virtual networks, a resource can be re-used for multiple networks or multiple resources can be aggregated for virtual resource. However, to manage these virtual resources effectively there needs to be a management system.

A key issue in the management of virtual networks is the development of a common control space, which has autonomic characteristics and enables heterogeneous network technologies, applications, and network elements to interoperate efficiently. Management applications need to be adaptive to a rapidly changing environment with respect to specific network properties, and service or user requirements, as examples. This implies that management applications and network entities should be supported by a platform that collects, processes, and disseminates information characterizing the underlying network. An increased awareness regarding the properties and state of the network can bridge the gap between high-level management goals and the configuration that achieves them. In this respect, we consider an infrastructure that manages both information flow and processing within the network as an important stepping-stone towards this objective.

Key design requirements of an information management infrastructure are: (a) information collection from the sources (e.g., network devices), (b) information processing that produces different information abstractions, and (c) information dissemination to the entities that exploit that information. It is common that such design approaches aggregate information using aggregate functions. Consequently, real-time monitoring of network parameters may introduce significant communication overhead, especially for the root-level nodes of the aggregation trees. Information flow should adapt to both the information management requirements and the constraints of the network environment, one example being: changes in the information collection configuration.

Such a management system should have to include a *management overlay* that collects, processes, and disseminates information from and to the network entities and management applications, acting as an enabler for self-management and self-awareness functionality. For example, this management overlay could regulate the information flow based on specific characteristics of the network environment (such as the network topology) and performance requirements (such as low data rate). To feed all the required and relevant information into the management overlay there needs to be a monitoring system that can collect such data from probes or sensors in the network environment and in the virtual resources. It can then report that data into the management overlay.

Appendix A provides an overview of main network resource management protocols.

2.1.4 Resources System Model

A principal consideration of resource management systems is the efficient assignment of resources to customers. The problem of making such efficient assignments is referred to as the *resource allocation* or *scheduling* problem and it is commonly formulated in the context of a *scheduling model* that includes a *system model*, which is an abstraction of the underlying resources. The system model provides information to the allocator regarding the availability and properties of resources at any point in time. The allocator uses this information to allocate resources to tasks in order to optimize a stated performance metric. This paradigm is useful for *high performance applications*, which have tight constraints. Efficient scheduling of resources is critical in meeting these constraints.

In a distributively owned environment, the owner of a resource has the right to define its usage policy, which may be very sophisticated. For example, the policy may state that a job can run on a workstation only if the it belongs to a particular research group, or if it is run between 6 p.m. and 6 a.m., or if the keyboard hasn't been touched for over fifteen minutes and the load average is less than 0.1. Distributed ownership makes it impossible to formulate a monolithic system model. There is therefore a need for a resource management paradigm that does not require such a model and that can operate in an environment where resource owners and customers dynamically define their own models.

2.1.5 Slice embedding solutions

Network virtualization provides a novel approach to running multiple concurrent virtual networks over a common physical infrastructure. F. Esposito, I. Matta and V. Ishakian [86] provide an extensive survey on slice embedding solutions for distributed service architectures. There exist coexisting meanings of virtualized networks, i.e. virtual private networks (VPNs), overlay networks, and virtual networking. In VPNs, virtualization is limited to the physical network layer; in overlay networks, virtualization is limited to the end-hosts. Network virtualization introduces the ability to access, manage and control each layer of the current Internet architecture in the end-hosts and the network layer at the same time, and construct virtual network slices, which may be characterized by fundamentally different protocol architectures.

Slice is defined as a set of virtual instances spanning a set of physical resources of the network infrastructure. By physical resources, we mean mainly processes, storage capacity, computational resources, and physical links. The slice embedding problem is essentially a closed-feedback system, which includes three main steps, i.e., resource discovery, virtual network mapping and allocation, as illustrated in Figure 1.

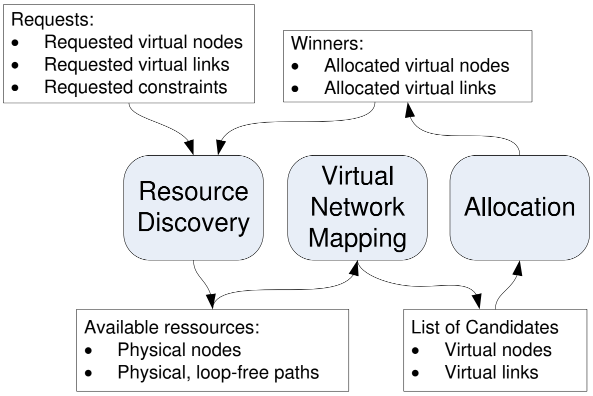


Figure 1 - Slice embedding problem.

Resource discovery involves resource awareness and monitoring. It receives from the users requests for slices in terms of virtual nodes, virtual links, and constraints. Resource discovery results in the set of available physical resources, which maximizes a given notion of utility, e.g., regarding the distance of the resources to the given set of requested constraints.

Virtual network mapping involves the complex, NP-hard problem solution of mapping the demanded resources to available resources. It outputs a list of candidate mappings of the requested nodes to physical nodes and the requested virtual links to candidate physical paths. A mapping is valid if all constraints of the virtual networks are satisfied. Such constraints are the number of CPUs, memory size, physical location of the node, or delay, jitter, bandwidth of virtual links. The objective function used in the optimization problem of network mapping may also include revenues, which the system will get if the virtual network requests of specific users are mapped to given resources.

Allocation is the final step, where the virtual resources are indeed assigned to the physical resources considering the constraints of the physical infrastructure and user priorities.

These three phases of the slice embedding problem have interactions among them. Many authors deal with combinations of these phases, but a unified description of the optimization problem is first introduced in [86].

Slice embedding problems can be categorized based on the used constraint types, their dynamics and type of admission control.

Regarding constraint types in the requests, users may or may not express their preferences about node and link constrains and inter-group or geo-location constraints. The model may consider constraints in series or simultaneously, leading to local or global optimum solutions.

Each phase of the slice embedding problem may have different dynamics. E.g., the status updates of each resource may be collected periodically or on demand. The virtual network mapping phase may statically map demands to candidate resources or may move the mappings using path migrations or rerunning the mappings. Mapping may focus only on nodes or links at a time, or simultaneously on both nodes and links. Allocation may be dynamic as well, users may be swapped in or out to achieve certain QoS levels.

At the physical infrastructure level, physical resources are limited; therefore, admission control is necessary to avoid violation of resource guarantees for existing virtual networks. Admission control is called tentative admission control, or soft reservation, if the system issues tickets and it is without guarantee that tickets can be exchanged later with resource. On the other hand hard resource allocation guarantees can be provided if the allocation scheme enforces admission to the users by monitoring the state of resources.

A problem related to resource discovery and allocation is the resource description problem. References in [86] involve a set of different languages, interfaces to publish and search for resources as well as data structures for organizing such information (e.g., RSpec [93], OASIS [92]).

Depending on the use cases, the lifetime of slices may vary from seconds, e.g., in case of cluster-on-demand application) to years (in case of virtual network hosting or leasing). In slices having short lifetime, the slice creation and embedding time, and slice removal time are not negligible.

Dynamic approaches to network mapping and allocation are also an interesting area, due to the varying lifetimes and constraints of embedded slice requests. It is evident that static resource assignment for multiple virtual networks customized to particular applications can lead to underutilization of physical resources.

There exist several dynamic network mapping and allocation approaches in the literature, Lu and Turner [89] apply iterative reassignment of virtual links. Yu at al. [90] take into consideration virtual resource migration operations. Fan and Ammar [91] apply dynamic topology mapping for virtual networks, without considering node constraints.

An interesting proposal to the dynamic network mapping problem is the Dynamically Adaptive Virtual Networks for a Customized Internet (DaVinci) architecture [87]. The DaVinci architecture assumes N different virtual networks, each optimizing their network flows (the bandwidths of virtual paths) based on their proper utility functions. The dynamism of this approach lies in the periodic reassignment of physical bandwidth to the hosted networks. For this purpose, there is a main optimization problem, which maximizes the aggregate utility for the infrastructure provider. The most significant assumptions in this model are that physical links are aware of the performance objectives of hosted virtual networks, which may not be possible in existing systems.

Optimization theory, i.e., maximization of certain utility function, may not be the proper method for allocation of slices when there are multiple competing entities, which may allocate resources to slices. For such scenario,s game-theoretic approach may be applied during the allocation phase, such as the colocation game proposed by Londono et al. in [88].

When a service must be provided across multiple provider networks, centralized coordination of virtual resource management assuming complete knowledge of the substrate network becomes invalid. Furthermore, providers are not happy to share traffic matrices and topology information with a decision entity, which also may hinder the usage of previous solutions. There exist several proposals for distributed virtual network mapping solutions, which are appropriate in these scenarios. In some solutions [94][95] a centralized authority is still responsible for partitioning the slices and the orchestration of the mapping of virtual resource demands to physical resources.

Houdi et al. [96] define a fully distributed virtual network mapping problem, where three algorithms are running concurrently at each substrate node, i.e., (1) capacity node sorting and (2) shortest path tree algorithms providing up-to-date information on the topology and available capacities of nodes and links, and the (3) main mapping algorithm. In [97], Chowdhury et al. describe a policy-based inter-domain mapping protocol, PolyVine, providing hierarchical addressing schemes for substrate nodes, advertising availability and price information via a Location-Awareness Protocol (LAP). Esposito et al. [98] propose an auction-based distributed mapping solution, where a consensus-based auction guarantees convergence and approximation bounds on the optimality of the embedding.

2.1.6 Cloud resource management

Cloud service providers are often faced with large fluctuating loads, which must be efficiently served. In some cases, when the load can be predicted, resources can be provisioned in advance. On the other hand, for unpredicted spikes auto-scaling is the best solution, where there is a pool of resources that can be allocated or released based on demand. There should also be a monitoring system, which allows e.g., a control loop to decide in real time to reallocate resources. Auto-scaling is supported by Platfrom-as-a-Service (PaaS) type services, such as Google App Engine, but is complicated in case of Infrastructure-as-a-Service (IaaS) type services due to the lack of standards [99].

Two main types of scaling exist: horizontal and vertical scaling. Vertical scaling keeps the amount of virtual machines (VM) of an application constant, and scales up the amount of resources allocated to the VMs, optionally, by migrating the VMs to a more powerful host machine. Horizontal scaling is more widespread. It increases the number of VMs allocated for the service, which often leads to the increase of the communication bandwidth of the application.

An application or service should be designed to support scaling. Modularly divisible applications only support vertical scaling, arbitrarily divisible applications support horizontal scaling, hence can be scaled up and down based on the incoming load.

Cloud resource management mechanisms typically cover subsets of the following tasks: (1) admission control, to prevent violation of services in progress by accepting additional workload; (2) capacity allocation, to allocate resources for service activations. When the states of individual systems change rapidly, locating resources subject to multiple global optimization constraints is a complex problem. (3) Load balancing and (4) energy optimization, by, e.g., concentrating the load to the minimum number of physical servers, and switching the others to standby mode. (5) Quality of service guarantees, which are most difficult to address, and most critical for the future of cloud computing. There are four basic mechanisms for the implementation of cloud resource management policies, i.e., control theory, machine learning, utility-based optimization and market-oriented mechanisms.

Many papers deal with the implementation of different cloud resource management policies including [100][101][102]. Several papers are concerned with Service-Level Agreements and QoS. E.g., [103] covers SLA-driven capacity management and [104] introduces SLA-based resource allocation policies. Dynamic request scheduling of applications subject to SLA requirements is presented in [105], and QoS in clouds is analysed in [105].

2.1.7 SDN-based resource management

The Software-Defined Networking (SDN) [161] is a new network architecture paradigm, where the control plane is completely decoupled from the data plane. The goal of SDN is to make “programmable network”, to allow applications to interact directly with the network in a two-way cooperation: the application informs the network of the desired behavior, the network informs applications about its capabilities.

The Software Defined Networking combines several technologies that decouple and open network control and management planes to facilitate their participation in broader orchestration structures via API. These API also facilitate the development of a new rich set of applications and network services.

The main promise of SDN architecture therefore lies in accelerating deployment and reliability of network configurations. It can lead to a radical change in the network and cloud of operators: the provisioning becomes a matter of hours rather than days. The overall IT agility is therefore multiplied.

The main idea of the SDN architecture is to extract the control plane from the network. In this way, rules and forwarding decisions are fully delegated to a central body: the SDN controller. It has complete visibility of the flows in transit in the network nodes of its domain. It defines according to the algorithms positioned by the administrator, the behavior to be applied to each stream: forwarding, tagging or blocking packets… An SDN architecture is based on a specific central “hypervisor”: the SDN controller, which is the junction between the north applications and network equipment in the South. The South interface can rely on the OpenFlow standard or others.

An SDN controller will act within its SDN domain; the east/west interfaces allow controller-to-controller communications to ensure E2E flow behaviour.Figure 2 shows a generic SDN architecture:

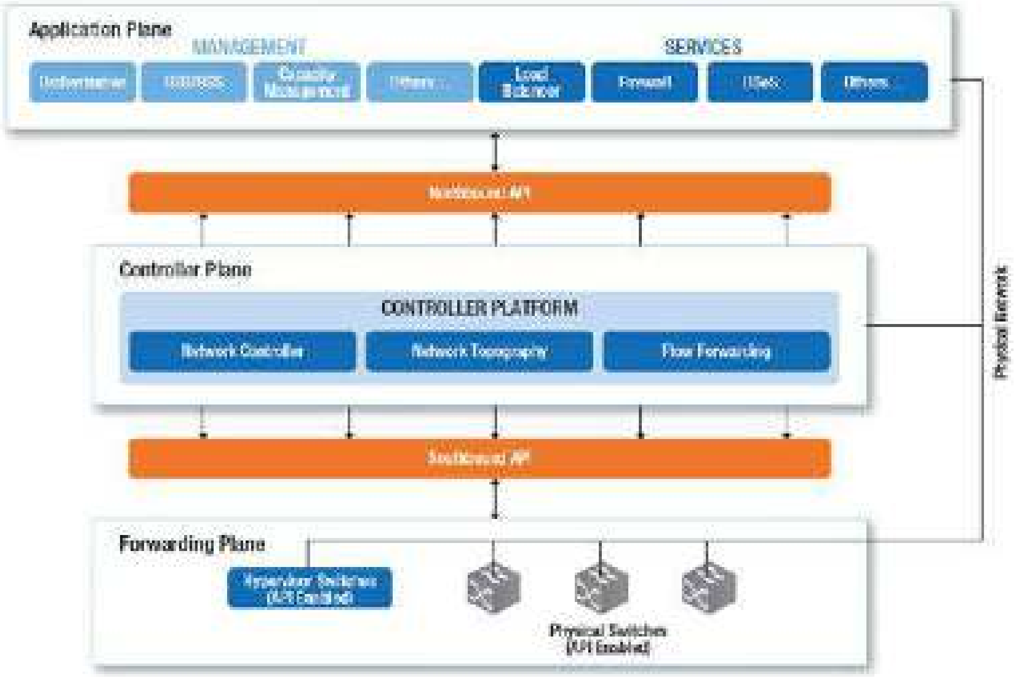


Figure 2 - SDN architecture.

SDN architecture as detailed in the figure above is based on a three layer architecture:

Application plane

SDN applications and /or cloud orchestrators interact with the SDN controller via open APIs. Note that an application must be made "SDN compatible" by integrating these APIs.

Controller plane

This is the SDN controller, which is the junction between the north applications and network equipments in the South. It translates requests made by applications in “language” understandable by the network components such as switches, routers, wireless AP, etc., whether physical or virtual. The SDN controller features a number of directives that control the behavior of network elements of the underlying network within its domain so that the network will provide desired network operations.

The controller provides as well performance and anomaly management functions via SNMP and other standard protocols.

The controller manages the configuration of compatible devices with with protocols such as OpenFlow to provide network topology, transmission, quality of service and link management.

Infrastructure layer

It contains the network nodes that exchange instructions and information with the control layer through dedicated protocols. Thus, in a SDN world, network nodes do not have to implement routing protocols, only a link to the controller issuing its decisions in real time. It is therefore a quite big simplification change to nowadays architecture.

An example of such design is the Opendaylight controller as shown is the figures below

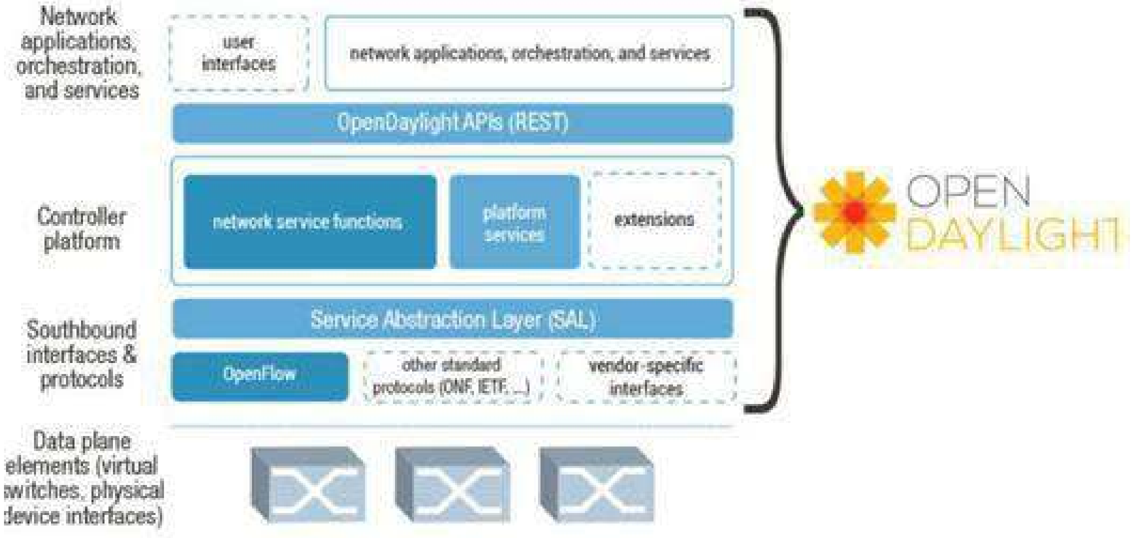

Network applications, orchestration, and services
user interfaces
network applications, orchestration, and services
OpenDaylight APIs (REST)
Controller platform
network service functions
platform services
extensions
Southbound interfaces & protocols
Service Abstraction Layer (SAL)
OpenFlow
other standard protocols (ONF, IETF, ...)
vendor-specific interfaces
Data plane elements (virtual switches, physical device interfaces)
OPEN DAYLIGHT

Figure 3 – OpenDaylight SDN controller architecture.

In the following section, we describe a video streaming service, where SDN resource management will provide management of network bandwidth and delivery of video streams.

2.1.8 Video streaming application

Video streaming application called BVS (Bull Vidéo Service) is a convergent video transcoder and streamer which performs on-the-fly and off-line video conversion and multi-protocol delivery.

Main caracteristics of the plateform are as follow:

- Support of a wide range of media codec and file formats on CBR or VBR input and output streams,
- Caching capabilities avoiding multiple transcoding of the same content allowing higher session capacity,
- External API to allow access from external application,
- High scalability by modular design.

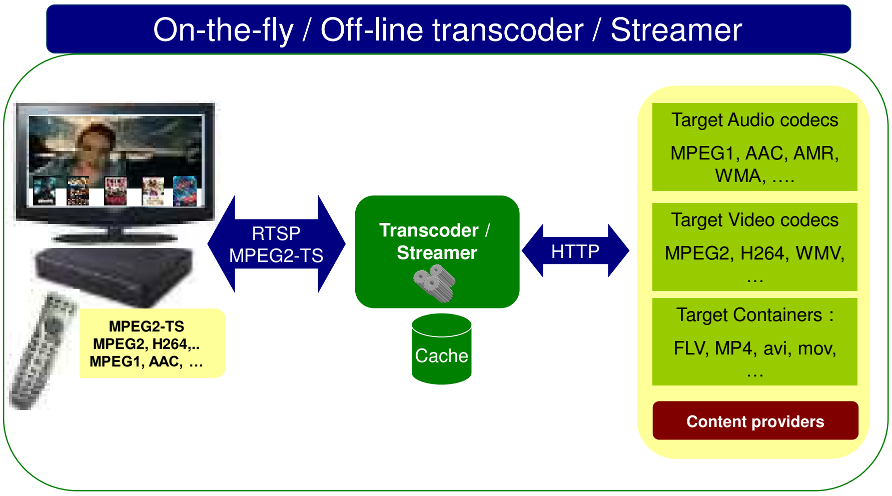


Figure 4 – BVS Video Service.

2.1.8.1 Scope and context

Video streaming has greatly evolved during the past years. Fisrt solutions were “bandwidth driven” without adaptative streaming mechanism.

The different steps were seen as follow:

- Content servers were providing a catalog of prepared videos with different bitrate encoding,
- The end-users were selecting a given video in this catalog. Video application was deciding a given bitrate (quality) based on end device characteristics. Once chosen, a given video stream was used during the whole streaming. In case of lack of bandwidth during streaming, video was freezing.

The result of such behavior is an uncontrolled user experience.

Nowadays, adaptative streaming has been introduced. Delivery servers still provide a set of prepared multi-rate video formats and adaptive streaming protocol is used by the end-user device player to decide which video stream is played among the available bitrates, depending on observed network bandwidth during video playing and end user cache.

The video is still “bandwidth driven” but streaming is more tolerant against bandwidth variation. Video quality may vary during streaming (adapting to available bandwidth), either for worse or better, video should never freeze.

A typical architecture is shown in Figure 5. The end-user experience is better, but a guaranteed quality SLA may not be reached, as the application has no way to define/control the best path on the network.

Current limitations seen by such solution are as follows:

- Video quality delivery is still not fully predictable
- Delivery server scalability is not met: several video delivery platforms are required, running on top of virtual machines and in several data centers in the cloud. We require the ability to select on the fly the most adequate data center for video delivery,
- Management of network bandwidth and delivery is not met: video delivery control is required. SDN networks provide APIs to manage the flows in the transport network.

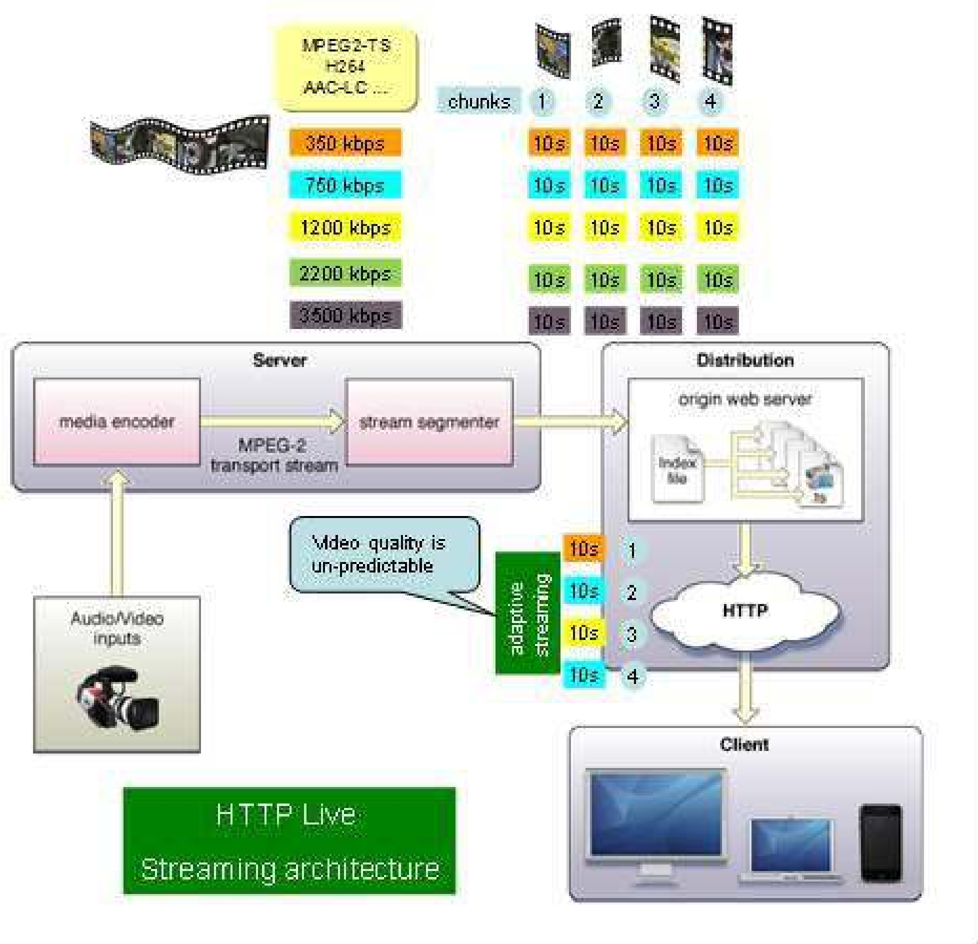


Figure 5 – Video service architecture.

2.1.8.2 Use of SDN based capabilities

Application remains the same as adaptive streaming. A new technical solution is to enable interaction between application servers and the SDN controller so that distribution location and streaming paths are managed within a SDN domain. The following steps describe the scenario:

- End-user is asking for a video inside a catalog, application servers will analyze the request to :
  - decide which set of multi-rate video to serve (min/max bandwidth depending on SLA and network inputs),
  - ask the SDN CTL based on requested bandwidth to define the optimal path.

Figure 6 depicts the communication flows of the application and the controller. To achieve such behavior we will focus our research on the following option:

- BVS relies on an SDN controller feature called Affinity service (in case of OpenDaylight controller). The controller is responsible for the computing and the provisioning of the path.

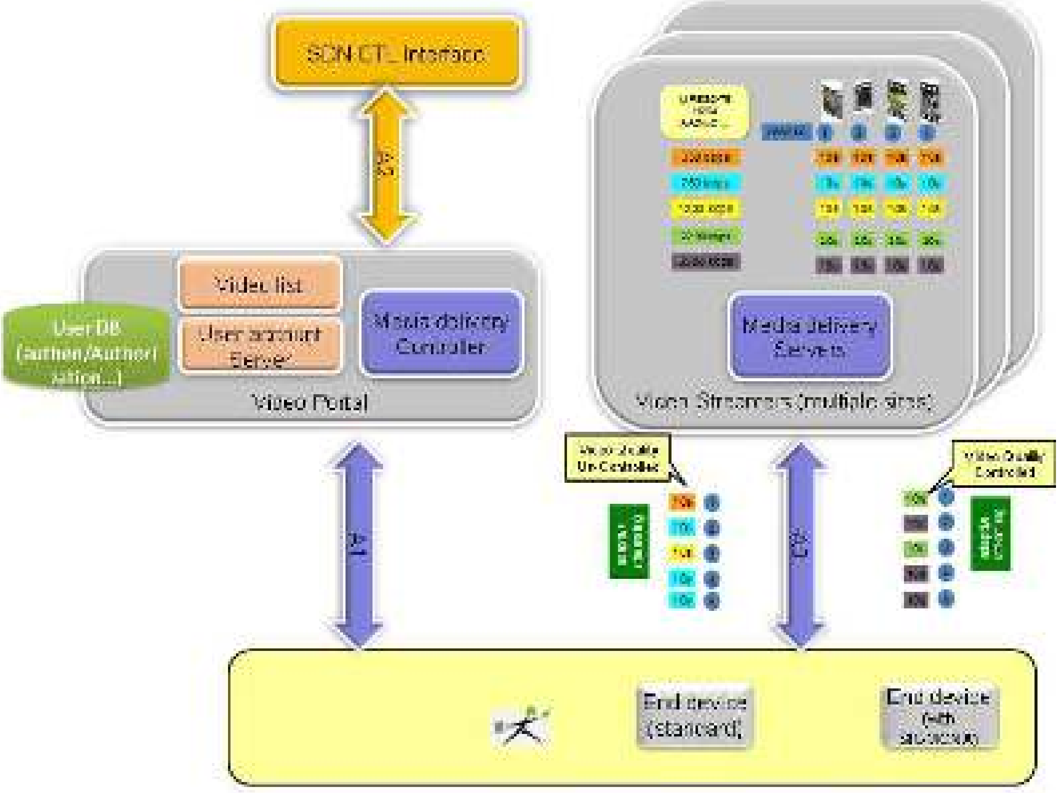

SDN CTL_Interface
Video list
User account Server
Media delivery Controller
User DB (authen/Authori sation...)
Video Portal
Media delivery Servers
Video Streamers (multiple sites)
Video Quality Un-Controlled
Video Quality Controlled
End device (standard)
End device (with SIGMONA)

Figure 6 – BVS & SDN communications.

The Affinity concept is based on a model in which SDN controllers dynamically provision the network infrastructure to satisfy workload affinities, lead by external applications. When enabled it allows configuring flavored path with the following data models.

- Affinity group that represents end points with L2/L3 addresses,
- Affinity link that represents a set of unicat flows between two end points,
- Affinity attributes that define "policies" to determine optimal way points routing.

Affinity service is currently limited to a single L2 domain and will be improved in the next Opendaylight releases. Figure 7 illustrates the Affinity Service in OpenDaylight controller. The Affinity Service enables applications to model their network requirements at the controller. Affinity group is a set of enpoint IDs, such as L2/L3 addresses. Affinity links is a set of unicast flows between two affinity groups, which can be uni- or bi-directional. Affinity attribute is a set of policies, primarily determining the network path to assign, taking into account performance, service quality, security or other requirements. Different policies are, e.g., connectivity, least hop count, waypoint routing through single network service point, firewall etc.

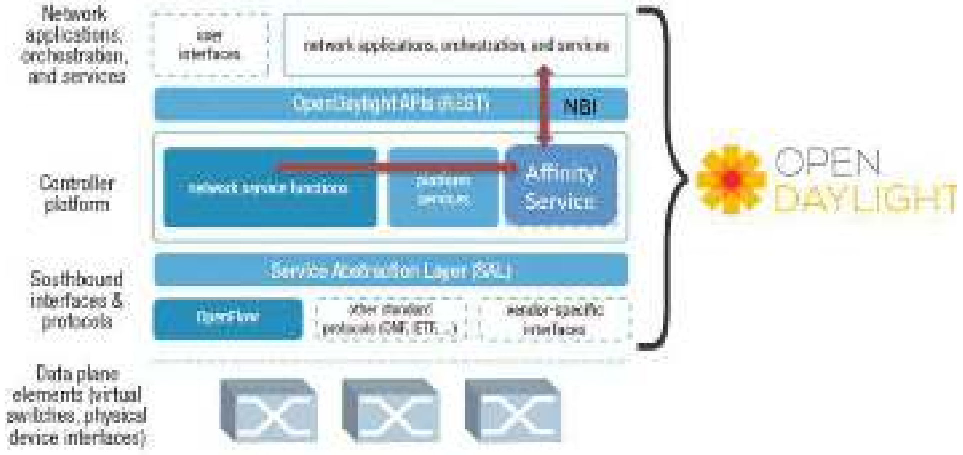

Network applications, orchestration, and services
user interfaces
network applications, orchestration, and services
OpenDaylight APIs (REST)
NBI
Controller platform
network service functions
platform services
Affinity Service
Southbound interfaces & protocols
Service Abstraction Layer (SAL)
OpenFlow
other standard protocols (ONF, IETF, ...)
vendor-specific interfaces
Data plane elements (virtual switches, physical device interfaces)
OPEN DAYLIGHT

Figure 7 – ODL SDN affinity service.

2.2 Traffic management

This section discusses the state-of-the-art of traffic management in mobile networks using SDN, NFV and cloud-service concepts. The topics cover dynamic routing, service chaining, application-layer traffic optimization and QoS enforcement.

2.2.1 Definition of traffic management

Traffic management methods may be both necessary and warranted in the operation of broadband networks because of overbooking, i.e., the network capacity requirements of the acquired services generally far exceed the available network capacity. Traffic management methods can mitigate the negative effects of congestion and can contribute to a more fair distribution of scarce network resources among users. Moreover, traffic management allows service providers to define service features.

Regulation, in European countries, in the US etc, requires transparency of the network, no blocking of content and no unreasonable discrimination of content. However, some users or applications (especially in content delivery) require Quality of Service (QoS) guarantees and data discrimination. Therefore, the regulations of such countries require from providers that Quality of Service criteria shall be defined in the Quality of Service Decree in a detailed manner based on the establishment of the service, the error ratio, availability, troubleshooting, etc., and various quality target values depending on the nature of the service. Moreover, other QoS target values may also be defined by the services, which are not included in the Quality of Service Decree. The service provider must define quality of service commitments in the General Tems of Conditions [1].

Traffic management can be realized in many ways, all targeting the increase of efficiency of resource utilization and the provision of contracted service characteristics. It includes, e.g., pricing, renegotiation of contracts, call admission control, resource allocation, traffic steering, packet scheduling and traffic priorization, multicast addressing, gating control, and policy management.

The traffic management work in SIGMONA project focuses on new components in the SDN application layer / SDN overlay, as well as the management and monitoring layer, for the realization of service chaining concepts, resource allocation, traffic steering, packet scheduling and traffic priorization, and QoS provision, on top of partly SDN-based transport network and assuming partly virtualized mobile network functions.

QoS includes monitoring and recording of parameters related to the establishment, retention and quality of the connection. Cooperation with fault (maintenance) management to establish possible failure of a resource, also with configuration management in order to change routing and load control parameters for links.

2.2.2 Possible traffic management methods for SDN

SDN has the potential to accelerate network innovation by decoupling the control plane and data plane. With this architecture, software can be developed independently of the hardware. The control plane of SDN is centralized and sends the control information to the data plane. This architecture provides a view of the entire network enabling the user to optimize the entire network. SDN can reduce network complexity, hence it is suitable for sophisticated environments such as a mobile network [172][173]. One of the potential main components of the SDN concept is OpenFlow (OF) [174].

All the control functionality is given to a centralized controller such as NOX [175], Maestro [176], Beacon [177] and Floodlight [178] in the initial design and implementation of SDN because of the simplicity and flexibility. However, a single controller may not be enough to manage a network with a large number of data plane elements, as the size of the network grows. Contrary to a centralized design, a distributed network operating system can be scaled up to meet the requirements of potentially any environment, from small to large-scale networks. Onix [179], HyperFlow [180] and Kandoo [181] are examples of distributed controllers.

Existing wireless networks suffer from inflexible and expensive equipment, complex control-plane protocols, and vendor-specific configuration interfaces. Compared with wired networks, wireless networks have some unique features and face significant scalability challenges. For example, because users are always moving in the wireless networks, there will be a large number of state updates generated from the data plane, which would create big pressure on a central controller. In addition, the average response latency would also increase sharply when a set of base stations communicate with one remote controller concurrently. Thus, some efforts have been done to apply SDN concepts to wireless networks in order to simplify the design and management. An early attempt to develop a wireless SDN platform with OpenFlow and NOX called OpenRoads that separates control plane from the datapath is designed in [75]. The OpenRoads allows several different experiments and services to run simultaneously over one physical network. Bansal et al. [182] propose OpenRadio, a platform that is quite close to OpenFlow in the sense that it aims at achieving a programmable data plane in cellular networks. OpenRadio aims to provide an infrastructure to update base stations of wireless systems via software. Without this approach, devices must be collected so that the software can be manually updated. This frequent hardware collection is expensive and network software updates are more adequate. [183] propose an SDN architecture with local control agents, which is designed for handling this problem. It is claimed that SDN can simplify cellular networks and lower management costs in this study. In the proposed architecture, the local software control agent can make simple decisions for a single base station. The centralized controller should express and interpret flows and cellular resources with high-level abstractions rather than IP addresses or physical identities. To improve the performance of the control plane, some simple actions and policies are run on a local control agent. Unfortunately, the authors do not provide an architectural blueprint detailing their proposal; nor do they report experimental results.

In [84], the authors proposed an SDN controller for cellular networks (CellSDN), which is logically centralized, and realizes high-level service policy by directing traffic through a sequence of data plane nodes. In [85] the authors propose a new architecture called SoftCell for the cellular core network based on inexpensive access switches, middleboxes and a centralized controller composing the data path for each user flow through a set of highly distributed middlebox functions. SoftCell can be thought as the improved version of CellSDN. [184] proposed to use SDN principles to redesign the radio access network and called the study SoftRAN. It is therefore complementary to SoftCell which focuses at redesigning the core network instead of radio access network. In SoftRAN, all LTE network are controlled in a centralized way: all the base stations are abstracted as virtual elements and managed by the logically central controller. [185] proposed an OpenFlow-based control plane for LTE/EPC architecture, which particularly splits between the control and data forwarding planes related to the Serving Gateways (SGWs). They showed that this architecture easily ensures the on-demand connectivity service even in critic situation such as network equipment failure and overload situations. [186] and [187] try to define, model and solve the problem of applying virtualization, SDN decomposition or a combination of both concepts on the mobile core gateways. [190] and [78] proposed to virtualize the control plane side of the entities of the Evolved Packet Core (EPC), so they can run in a cloud environment and use a simpler and flatter network architecture in the data plane, following an SDN approach to manage the forwarding and allowing to benefit from enhanced flexibility. They replaced the data plane of the EPC core by OpenFlow switches. In [188] and [189], an SDN based LTE framework is proposed. The aim of [188] is to provide efficient content delivery services in the mobile environment and to support easy network management. In [189], transport is simplified with SDN switches and the control plane is simplified by merging LTE network elements such as MME, S/P-GW into a single network component.

SDN has also been integrated to the very dense heterogeneous wireless networks. These DenseNets have limitations due to constraints such as radio access network bottlenecks, control overhead, and high operational costs [192], [193]. A dynamic two-tier SDN controller hierarchy can be adapted to address some of these constraints [192], [193]. Local controllers can be used to take fast and fine-grained decisions, while regional (or “global”) controllers can have a broader, coarser-grained scope, i.e., that take slower but more global decisions. In such a way, designing a single integrated architecture that encompasses LTE (macro/pico/femto) and WiFi cells, while challenging, seems feasible. OpenRAN, an architecture for software-defined RAN via virtualization was proposed in [194] for heterogeneous wireless networks. In [195], a heterogeneous scenario was proposed, where Machine to Machine (M2M) and LTE interoperation was examined. SDN has been used to make LTE cellular network much simpler to manage and reconfigure, by introducing new features, and interoperating with other technologies, in particular with M2M communications equipment. Indeed, SDN will be a key issue also in future fifth-generation cellular networks [196].

As networks become more complex and traffic diversity increases, there is the apparent need to manage the traffic carried by the network. The goal of traffic management is to decide how to route the traffic in a network in order to balance several objectives such as maximizing throughput, balancing the link utilization across the network, controlling the bandwidth allocated to competing flows in a fair manner, minimizing latency and ensuring reliable operations when traffic patterns change or parts of the network fail. In the literature, the people have different architectures to apply SDN into the cellular networks as given above. However, they do not say anything on how to manage the network traffic so there is still no standard mechanism for using these contexts in a software-defined system.

Traffic management has received a great deal of attention within the OpenFlow/SDN community. Agarwal [78] has considered the traffic engineering problem that is motivated by scenarios where SDNs are incrementally deployed in an existing network. In such a network, not all the traffic is controlled by a single SDN controller. There may be multiple controllers for different parts of the network and also some parts of the network may use existing network routing such as Open Shortest Path First (OSPF) which is most widely used path selection protocol that assigns weights to links and computes the shortest path across the network. They tried to answer the question if it is still possible to do effective traffic engineering when all the traffic in the network cannot be controlled centrally by a single SDN controller. They formulate the SDN controller’s optimization problem for traffic engineering with partial deployment and develop fast Fully Polynomial Time Approximation Schemes (FPTAS) for solving these problems. The reason for solving the problem as an FPTAS instead of a standard linear programming problem is that the FPTAS is very simple to implement and runs significantly faster than a general linear programming solver especially on medium and large sized problems. [81] presents a novel SDN controller that classifies the network traffic types according to the heterogeneous Quality of Service requirements that the network data is separated into the Constant Bit Rate (CBR) based real-time traffic and File Transfer Protocol (FTP) based non-real time traffic. Some crucial traffic flow parameters such as packet delivery ratio, routing overhead and delay are also considered in this classification. [82] propose an efficient algorithm for joint backhaul traffic engineering and physical layer interference management for a large-scale software defined radio access networks. The proposed algorithm is a combination of two algorithms, the max-min weighted-MMSE (WMMSE) algorithm for minimum rate maximization and the Alternating Direction Method of Multipliers (ADMM) algorithm that is used to solve the multi-commodity routing problem in a distributive manner. The resulting algorithm is significantly more efficient than the subgradient-based methods. The proposed algorithm is scalable to large networks since all its steps can be computed in closed-form independently and in parallel across all nodes of the network. In [83], Chanda et al. present a content-centric network architecture, which is based on SDN principles and implements metadata driven services, such as metadata driven traffic engineering and firewalling, with the ability to parse content metadata at the network layer. Entropy theory is exploited to analyze the feasibility of predicting traffic dynamics theoretically for software defined cellular radio access network in [197]. The authors highlight in the paper that “entropy” offers a precise definition of the informational content of predictions by the corresponding probability distribution functions, and it possesses good generality because it makes minimal assumption on the model of the studied scenario. Thus, it is suitable to use the entropy approach for measuring the traffic predictability based on certain prior information from history or from neighboring cells.

2.2.3 Joint traffic and cloud resource management for service chaining in SDMNs

Existing cellular networks are starting to be insufficient in meeting the increasing traffic demand in part due to their inflexible and expensive equipment as well as complex and non-agile control plane. Furthermore, the popularity of cloud-computing based services and applications by over–the-top (OTT) providers has skyrocketed in recent years. For mobile operators, the existence of the OTT providers have resulted in a significant loss of new and existing revenue sources [198]. Mobile operators have been recently utilizing cloud-based approaches to implement new architectures that provide network efficiency, high QoE and shorter time to market for innovative services. Added network programmability is expected to boost the efficiency. Through a combination of Network-Enabled Cloud, Service Provider SDN, and Network Functions Virtualization (NFV) approaches, it is possible for the operators to remove the complexities of the topology and service creation, and accelerate the process of new service creation and delivery [199]

Today’s network control is concerned with not only the calculation of the end-to-end route for a given flow, but also, when necessary, an array of inline services, such as DPI, firewalls, Network Address Translation (NAT), etc. Inline services can be hosted on dedicated physical hardware, or on virtual machines. Service chaining, as depicted in Figure 8, is required to route certain subscriber traffic through more than one such service. There are still no protocols or tools available for operators to perform flexible, dynamic traffic steering. Solutions currently available are either static or their flexibility is significantly limited by scalability inefficiencies.

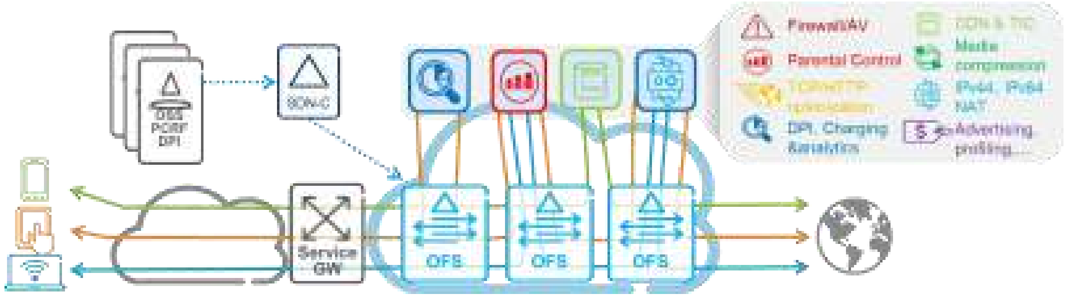


Figure 8 – Service chaining.

Given the rate of traffic growth, continued investment in capacity for fundamental cellular network functions such as the MME, P-GW, PCRF, etc as well as the inline services need to be managed carefully. Dynamic service chaining can optimize the use of extensive high-touch services by selectively steering traffic through specific services or bypassing them completely, which, in turn, can result in CAPEX savings owing to the avoidance of over-dimensioning.

Operators will not immediately shift to a network where all functions will be virtualized over cloud. New functionalities need to be in communication with existing network functions and enable a change over time. In addition to this, not every functionality will necessarily benefit from virtualization and cloudification. Therefore, there will be various different set-ups as depicted in Figure 9.

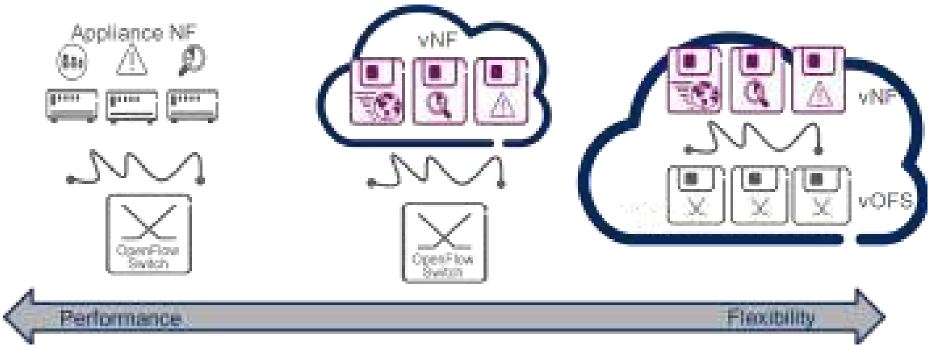


Figure 9 –Different set-ups of non-virtualized, virtualized mobile network.

Greater control over traffic and the use of subscriber and flow-based selection of virtualized network functions and inline services can lead to the creation of new offerings and new ways to monetize networks. Dynamic service (both virtualized network functions and inline services) steering enables operators to realize scalable network function components in the cloud while providing the capability to offer subscribers access to products such as virus scanning, firewalls and content filters through an automatic selection and registration portal. This concept of dynamic service chaining for LTE networks form the basis of Ericssons research thrust in SIGMONA and is built on SDN principles.

There is no existing body of work that jointly and dynamically optimizes the cloud realization of functions and services and a service chaining route for a given network flow. Related work until now concentrates on efforts of either cloud management or service chaining for SDN networks. Below, we summarize the related state-of-the art from the literature.

In [200], the authors introduce Dynamic-TEDI, a dynamic realization of TEDI, which is an indexing and processing scheme for shortest-path query answering, for cloud management in SDN networks. In the proposed architecture, the Cloud Controller interacts with the SDN Network Controller to describe an up-to-date view of the cloud topology, and the SDN controller in turn computes the shortest-path route. The route is dynamically adjusted when the Cloud Controller updates the topology map.

In [201], the authors propose to extend the scope of traffic management to the end-host network stack for joint host-network traffic management. The proposed architecture includes a logically centralized SDN controller, HONE (HOst-NEtwork) agents running on each host, and a module interacting with network devices. HONE performs monitoring and analysis on streams of measurement data in a programmable fashion.

An experimental SDN-based testbed is introduced in [202], where three data centers form a 125 km ring of single-mode optical fiber. The testbed shows an automatic triggering of live VM migration when the server utilization exceeds 75%. The open source application Ganglia is used for cloud management: monitor events such as server utilization and available memory and execute the migration or cloning of a VM. Upon a Ganglia trigger, the SDN controller automatically provisions the necessary switches in the network and target data center.

The authors in [203] propose an SDN-based cloud data center architecture where the SDN controller and cloud controller communicate for efficient flow- and vm-migration for optimum throughput and energy savings in the network. The dynamic migration of the flows as well as the VMs is based on the interaction between the two controllers, where the cloud controller provides information on VM-to-PM map, and the corresponding network description and the SDN controller provides the network monitoring information to one another. The paper introduces a traffic-aware flow migration with a dynamic rerouting algorithm for SDN.

In [204], the authors provide the results of an SDN testbed, where flow switching in a data center is combined with long distance optical networking so that rapid re-provisioning and reuse of network resources in response to changing application requirements becomes possible.

Hong et al. [205] predict the resource requirements such as CPU, bandwidth, memory, etc. across different applications in a cloud datacenter and dynamically allocate virtual machines to meet the service level agreements of applications. The work is claimed to be the first one that can adopt its resource prediction across different applications. However, service chaining is not considered. In [206], authors propose an SDN based architecture for the orchestration of dynamic resource chaining in cloud data centers. The computing capabilities provided by the servers and communication capabilities provided by the network switches are composed dynamically by the orchestrator to ensure less data exchanges between virtual machine deployments.

2.2.4 Application-layer traffic optimization in SDMNs

2.2.4.1 The ALTO problem

Application-layer traffic optimization (ALTO) problem arises when someone is concerned with better-than-random peer selection and/or optimization of rendezvous service for applications fetching distributed content. Typical fields where the ALTO problem occurs are peer-to-peer networks, content distribution networks and datacenters.

In peer-to-peer networks, peers can exchange pieces of information in an incremental way until the entire content is obtained. When a peer does not have a global view of the network, it may pick a candidate peer randomly, which may result in lower quality of experience (QoE).

CDNs distribute content and may cover large geographical areas. With the increasing demand for streaming video services, CDN servers/caches are deployed deeper in the network of internet service providers, including mobile network operators. CDN operators elaborated different technologies to direct the end users to the best CDN server or in-network cache of operators for appropriate level of QoE for the users.

A third area for ALTO problem is related to cloud services. Cloud services run on top of datacenters. Users should be served by the closest datacenter by a server loaded lightly enough. In case of virtual private clouds, the obtainment of proximity measures is more complicated because the service is provided through overlay networks; servers in the same virtual network may be located at different geographical locations.

Gurbani et al. [152] provide a good survey on existing solutions for the ALTO problem. ALTO solutions can be divided into two categories: (1) application-level techniques to estimate parameters of the underlying network topology and (2) layer cooperation. Techniques in 1) can be further divided to (i) end-system mechanisms for topology estimation, such as coordinates-based systems, path selection services, link-layer internet maps, and (ii) operator-provided topological information servoces, such as P4P [153], oracle-based ISP-P2P collaboration [154] or ISP-Driven Informed Path Selection [155].

The authors of [152] argue that these techniques have limitations in terms of abstraction of network topology using application-layer techniques, e.g., unable to detect overlay paths shorter than the direct path or accurately estimate multipath topologies, or do not measure all the relevant metrics for appropriate selection of the best endpoint. E.g., round-trip times do not reveal information on throughput and packet loss. Furthermore, topology estimations may converge slowly to the final result and application-layer measurements induce additional network resource utilization.

Hence, there is need of cooperation between application and network layers, where network operators should be able to provide network maps and cost maps representing distance, performance and charging related criteria.

2.2.4.2 The ALTO protocol

Application-Layer Traffic Optimization (ALTO) protocol has been specified by Alimi et al. [21] (IETF RFC 7285) in order to support interoperability between ALTO solutions of different vendors.

The two main information elements provided by ALTO service are the network map and the related cost maps. A network map consists of the definition of host-groups, but not the connectivity of host groups. The identifier of host-groups is called Provider-defined Identifer (PID). A PID may denote, e.g., a subnet, a set of subnets, a metropolitan area, a PoP, an autonomous system, or a set of autonomous systems.

A cost map defines one-way connections between the PIDs and assigns a cost value to each one-way connection. It also determines the metric type (e.g., routing cost) and the unit type (numerical or ordinal), as well as the network map name and version, where the PIDs are defined.

ALTO protocol is based on HTTP and uses a RESTful interface between the ALTO client and server. The protocol encodes message bodies in JSON [156]. Several JSON media types are proposed in [21], which realize required and optional functions. Required functions are the information resource directory, network and costmap request and responses. Optional functions of ALTO service are filtered network and costmap queries, endpoint property queries, etc.

2.2.4.3 ALTO-SDN use case

Gurbani et al. proposed in [151] the application of ALTO service in the SDN application layer. They argue that the ALTO protocol is a well-defined and mature solution that provides powerful abstraction of network map and network state that can be leveraged by distributed services in SDNs. ALTO hides unnecessary detail of the underlying networks without unnecessarily constraining applications, hence privacy of network information of network operators and content providers can be preserved.

A limitation of the application of ALTO protocol is that it does not specify network information provision service. Creation of network and cost maps in the ALTO server should be automated and policy driven. There is ongoing work for distribution of link-state and TE Information from BGP routers [157][158][159]. A similar approach should be adapted to SDN networks, i.e., the SDN controllers should be able to provide network information from which the ALTO server derives network and cost maps.

Xie et al. [19] prepared an IETF draft discussing possible use cases for the integration of ALTO service in SDNs. The benefits of the integration of ALTO network information service into SDNs are the following: ALTO becomes transparent for the end users or the service claimant entity (no deployment cost in the UE). Due to ALTO information, the ALTO client in the SDN controller can overwrite the initial peer selection decision of the service claimant entity (e.g. UE). Any flow can be dynamically selected for getting ALTO guidance and SDN controller provides built-in redirection mechanisms with flow rewrite rules. Furthermore, SDN controllers are aware of the topology and state of served network areas, hence can provide abstract network and cost maps to the ALTO server.

2.2.5 QoS provisioning in SDMNs

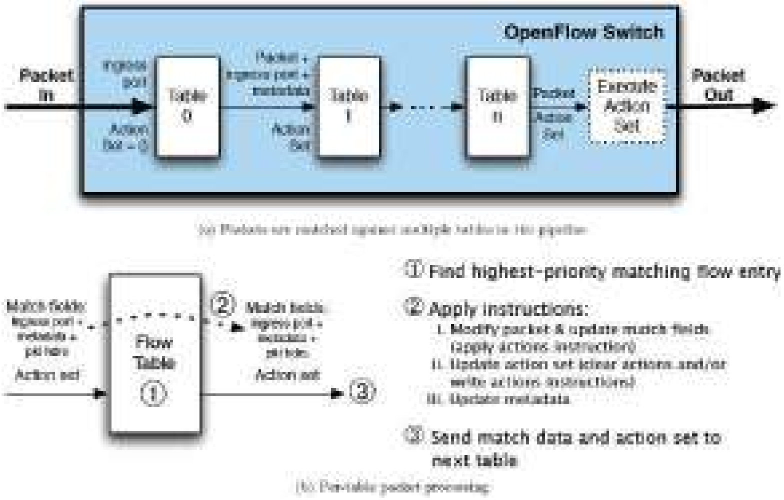
In current networks the decision logic and organization of network functions and protocols is distributed and multi-layered, enabling the evolution of each layer, separately. That makes the understanding and management of networks very complex, when network providers want to fulfill E-E connectivity and QoS requirements over different access networks for different services. SDN tries to hide this complexity, and introduces centralized control of the network.

Software-defined network domains could have the following advantages in EPC. In an SDN-based transport network, resources can be dynamically shared between services. Network slices can be easily created, modified and deleted, and rapidly adapted to the demands of user traffic.

When some network elements of EPC are deployed as virtual network functions in datacenters of the operator, SDNs can sustain connectivity between EPC elements, e.g., when Virtual Machines are “moving” between or within datacenters. This is possible e.g., with the virtual tenant network (VTN) concept of NEC, demonstrated within the OpenDaylight project. VTN allows the users to define the network with a look and feel of conventional L2/L3 network. Once the network is designed on VTN, it will automatically be mapped into underlying physical network, and then configured on the individual switch leveraging SDN control protocol. The definition of logical plane makes it possible not only to hide the complexity of the underlying network but also to better manage network resources. VTN achieves reducing reconfiguration time of network services and minimizing network configuration errors.

In SDN networking the Network Operating System (NOS) is in charge of controlling the SDN-capable networking elements (SDN switches) in a centralized way. The NOS has southbound and northbound APIs that allow SDN-switches and network applications to communicate over the common control plane provided by the NOS. In order to support multi-vendor environments for SDN switches and controllers, the southbound APIs must be standardized. OpenFlow (OF) protocol is widely applied standard for the southbound API.

The following figure illustrates the operation of an OpenFlow switch.


OpenFlow Switch
Packet In
Ingress port
Action Set = {}
Table 0
Packet + ingress port + metadata
Action Set
Table 1
Table n
Packet
Action Set
Execute Action Set
Packet Out
Match fields: ingress port + metadata + pkt hdrs
Action set
Flow Table
①
②
Match fields: ingress port + metadata + pkt hdrs
Action set
③
① Find highest-priority matching flow entry
② Apply instructions:
i. Modify packet & update match fields (apply actions instruction)
ii. Update action set (clear actions and/or write actions instructions)
iii. Update metadata
③ Send match data and action set to next table

(a) Packets are matched against multiple tables in the pipeline

(b) Per-table packet processing

Figure 10 - OpenFlow switch [7].

An OpenFlow switch contains multiple flow tables, which implement pipeline processing for incoming packets. Each table may contain flow entries. A flow entry contains:

- a set of match fields for matching the packets,
- priority for matching precedence,
- a set of counters to track packets,
- a set of instructions to apply,
- the maximum lifetime of the flow entry,
- the idle time before a flow entry is removed,
- cookie set and used by the controller as a group identifier of flows entries, enabling filtering queries for flow statistics, flow modification or flow deletion.

An instruction either modifies pipeline processing by sending the packet to another (higher number) flow table, or contains a list of a set of actions. Action set includes the actions accumulated during the packet has been processed by the flow tables. The actions are executed when the packet exits the processing pipeline. Possible actions are:

- output a packet on a given port,
- enqueue the packet to a given queue on a given port,
- drop packet,
- rewrite fields, such as TTL, VLAN ID, MPLS label,
- set other fields.

The second action can be applied in QoS service enforcement. It is called 'enqueue' in OF1.0 and 'set_queue' in OF 1.3 [7]. Its main purpose is to map a flow to a queue, but also can set up simple queues. The OpenFlow Management and Configuration Protocol (OF-Config 1.1.1) [8] defines API for configuration of SDN-switches.

OF 1.4 and OF-config 1.1 are able to set up queues, using two input parameters:

- Minimum rate: it specifies the guaranteed rate provided for the aggregate of flows mapped to this queue. It becomes important when the incoming data rate of egress port is higher than the maximum rate of the port.
- Maximum or peak rate: it becomes important when there is available bandwidth on the output port.

OF-config and OF do not support hierarchical queueing disciplines, which are necessary to implement standard or other per hob behaviors (PHB) specified for DiffServ architecture (described later).

Open vSwitch [207] is an implementation of a virtual switch with the aim of connecting virtual hosts in data centers. This implementation also is a proof-of-concept implementation for ONF.

Open vSwitch only supports two queueing disciplines: hierarchical token bucket (HTB), and hierarchical fair-service queue (HFSC) [7]. These queueing disciplines have much more configuration possibilities than minimum-rate and maximum-rate, such as the maximum queue size for HTB, or delay curves for real-time traffic in HFSC. QoS provisioning in SDNs using OF-switches is still in its enfance.

The advantages of queueing disciplines could be more leveraged if more queuing disciplines were available, the establishment of more than one level of QoS class hierarchies was possible, and more parameters of the queuing disciplines were reachable from OF or OF-config.

It is possible to configure hierarchical queueing disciplines in switches using their administration interfaces. OpenFlow is able to enqueue packets in queues of a multi-level queueing discipline hierarchy.

Therefore, more complex than the ones permitted by enqueue action can also be enforced using SDN-mechanisms. It is still an open question in SDN that which level of complexity of QoS configuration would be preferable.

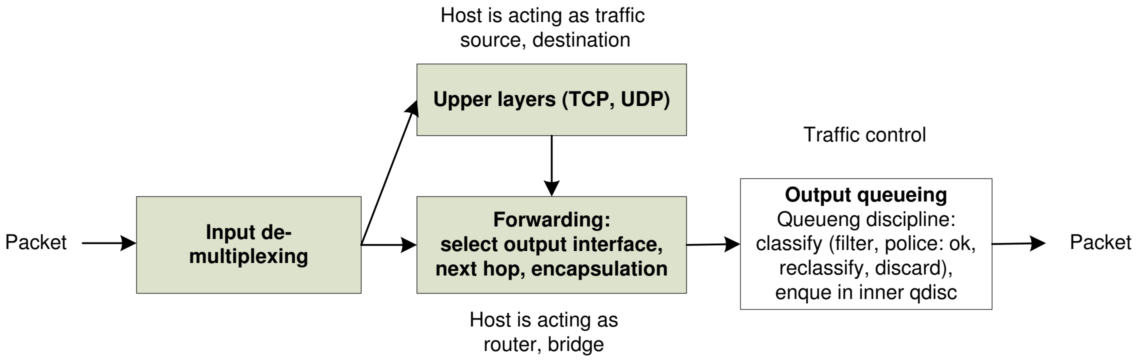
2.2.5.1 Metering in OpenFlow switches

The OF 1.4 specification contains requirements for the implementation of counters for flow tables, flow entrys, ports, queues, groups, group buckets, meters and meter bands. Some counters are mandatory; others are optional, as given in [7].

An OF controller can set meters in an OF switch to measure some metrics related to a flow, port, queue etc. It can set meter bands and appropriate actions if the actual measured metric falls into the meter band. Such actions could be Drop, realizing rate limiting, or DSCP remarking for assigning the packet to a new Behavior Aggregate. However, it is up to the implementation of the OF switch, whether these functionalities are available.

2.2.5.2 Overview of traffic control in Linux

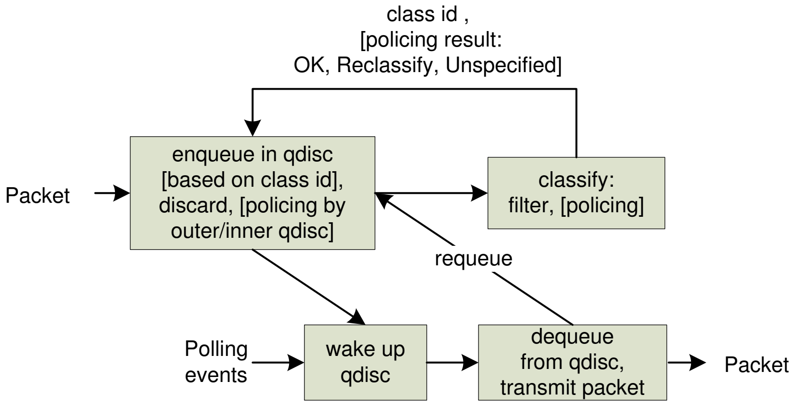
Figure 11 illustrates roughly how Linux kernel processes data received from the network. Incoming data is either directly forwarded to the network (i.e., the host is acting as a router or bridge) or to higher layers of the protocol stack (i.e., the host is the destination). Network data originating from or passing through the host is sent to the forwarding function. Forwarding is in charge of selection of output interface, next hop for the packets and encapsulate the packets into the appropriate format for the interface. Packets are then sent to the output interface, which has an associated queueing discipline enabling the priorization, scheduling, policing, and shaping of different traffic classes. Traffic control in Linux OS is realized in the output queueuing phase.



Host is acting as traffic source, destination
Upper layers (TCP, UDP)
Traffic control
Packet
Input de-multiplexing
Forwarding: select output interface, next hop, encapsulation
Output queueing
Queueng discipline: classify (filter, police: ok, reclassify, discard), enque in inner qdisc
Packet
Host is acting as router, bridge

Figure 11 – Processing of network data in Linux hosts.

Figure 12 depicts the output queueing process until the packet is sent to the network interface for transmission.



class id , [policing result: OK, Reclassify, Unspecified]
Packet
enqueue in qdisc [based on class id], discard, [policing by outer/inner qdisc]
classify: filter, [policing]
requeue
Polling events
wake up qdisc
dequeue from qdisc, transmit packet
Packet

Figure 12 – Output queueing.

Every interface has a queueing discipline (qdisc) associated. The default queueing discipline in Linux is typically the pfifo_fast queueing discipline. It is a classless qdisc defining three different FIFO queues with different priorities. IPv4 packets are mapped to queues based on the precedence values of the packets given in the ToS field.

If a packet is enqueued by a classful queueing discipline, then the packet must be classified. Classification is possible using filters, which enforce matching rules on specific fields in the headers of the packet, input port etc. Certain filter types can optionally provide policing. They compare the characteristics of matching flow to token bucket-based meters. This enables the verification of the fulfilment of traffic specification, i.e., whether the traffic source keeps the previously specified parameters, such as the max rate, min rate, burstiness etc. of the traffic flow. The outcome of policing may be acceptance, reclassification or discard of a packet. After a match and optional acceptance or reclassification, the packet is enqueued in the inner qdisc of the class. Depending on the number of levels of the class hierarchy, this enqueuing-classification loop may be repeated as many times as many class hierarchy levels are defined and the packet goes through these classification levels.

Dequeuing of packets from qdiscs is made in the opposite direction, from inner qdiscs towards outer qdiscs, until the packet is dequeued from the outermost qdisc. Dequeueing is never invoked directly, but polled by timers or by enqueuing events. When such events arrive in the qdisc, the qdisc wakes up and tries to dequeue the next packet from the corresponding queue. If there are packets in the queue then the following packet is sent to the interface. If the transmission fails, the packet may be sent back from the interface and requeued in the qdisc.

Traffic policing has multiple ways. One of them is when the filter decides on whether the packet is in or out-profile using token bucket, as described previously. Another option is that the inner or the outer qdisc decide to discard a packet from the inner qdisc when a new packet is enqueued.

Figure 13 illustrates a one-level classful queueing discipline. The packet arrives in the outer qdisc, which tries to classify it using a list of filters. The packet is typically discarded, if it does not match to any filter rule. After finding the class for the packet, it is enqueued in the inner qdisc associated with the specific class.

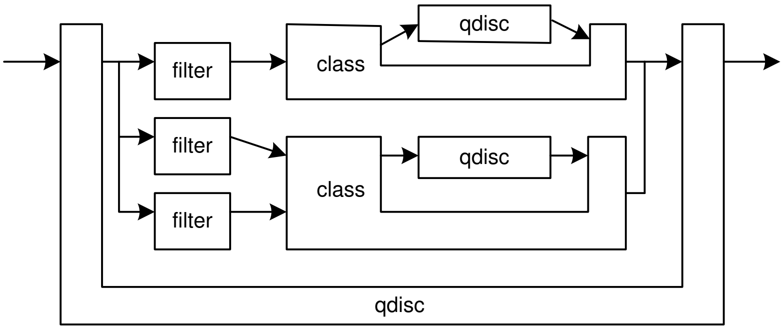


Figure 13 – A simple queueing discipline with multiple classes.

2.2.5.3 DiffServ QoS architecture in SDNs

In this section, we describe DiffServ QoS architecture, which can form the basis of scalable QoS service in SDN domains. Packet marking, simple scheduling techniques are supported by SDN switches (by flow rewrite, enqueue action, or switch specific QoS configuration capabilities). The fact of centralized control, flow statistics, furthermore the counter and metering functions of the switches could be used for traffic policing and bandwidth brokerage.

The DiffServ QoS architecture is defined in IETF RFC 2475 [9]. DiffServ provides QoS by assigning priorities to packets. Incoming packets have to be marked at the edge router of a DiffServ (DS) domain using the Differentiated Service Code Point (DSCP), which determines the per hop behavior (PHB), i.e., queuing and scheduling, of packets in the DS-routers within the DS domain.

Service guarantees are based on statistic factors and overbooking of routers may be possible, therefore, DiffServ can provide relative QoS, and requires bandwidth brokerage function or other admission control at the edge of the DS domain for correct operation.

The DSCP field is defined in RFC 2474 [10]. Standard per hop behaviors for Assured Forwarding (AF) and Expedited Forwarding (EF) are specified in RFC 2597 [11] and RFC 2598 [12], respectively. EF causes low delay, jitter and loss, and can starve other classes. AF defines four classes of priority queueing discipline, and three queues within each class for different dropping preference of packets. Default PHB means no guarantees, best effort traffic, that can be implemented, e.g., with stochastic fair queueing.

IntServ architecture requires signaling protocols for reserving resources along the path of the flow, hence packet do not need any mark indicating which class or priority they belong to. IntServ can provide guaranteed services. IntServ is a flow-based QoS architecture model, it does not scale well with the number of network nodes. DiffServ is a class-based QoS architecture model. It aggregates traffic flows entering the

DS domain according to the behavior, creating Behavior Aggregates, and reducing flow state information. Afterwards clear rules are created and preliminary installed at the routers for treating each of these classes.

DiffServ architecture is illustrated in Figure 14.

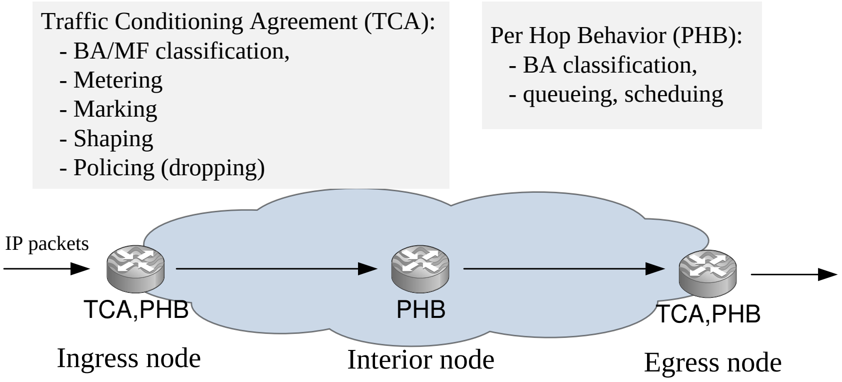


Figure 14 - DiffServ architecture.

Differentiated services are extended across a DS domain boundary by establishing a SLA between an upstream network and a downstream DS domain. The SLA may specify packet classification and re-marking rules and may also specify traffic profiles and actions to traffic streams which are in- or out-of-profile.

A traffic profile specifies the temporal properties of a traffic stream selected by a classifier. It provides rules for determining whether a particular packet is in-profile or out-of-profile. Different conditioning actions may be applied to the in-profile packets and out-of-profile packets, or different accounting actions may be triggered. In-profile packets may be allowed to enter the DS domain without further conditioning; or, alternatively, their DS codepoint may be changed. Out-of- profile packets may be queued until they are in-profile (shaped), discarded (policed), marked with a new codepoint (re-marked), or forwarded unchanged while triggering some accounting procedure.

Traffic conditioning control functions can be applied to a BA to comply with the SLA for each traffic profile. These may include metering, policing, shaping, and packet marking, as illustrtated in Figure 15.

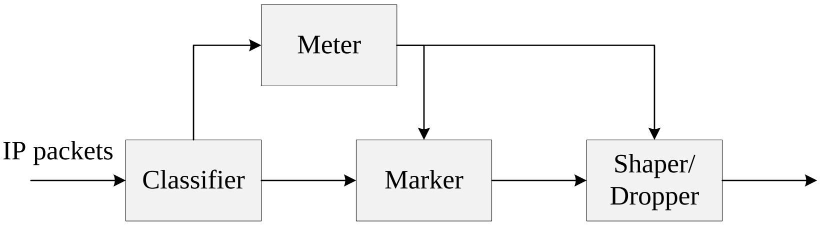


Figure 15 – Traffic classification and conditioning.

Packet classifiers select packets in a traffic stream based on the content of some portion of the packet header. We define two types of classifiers. The BA (Behavior Aggregate) classifier classifies packets based on the DS codepoint only. The MF (Multi-Field) classifier selects packets based on the value of a combination of one or more header fields, such as source address, destination address, DS field, protocol ID, source port and destination port numbers, and other information such as incoming interface. Classifiers are used to "steer" packets matching some specified rules to an element of a traffic conditioner for further processing.

Traffic meters measure the temporal properties of the stream of packets selected by a classifier against a traffic profile specified in a TCA. Packet markers set the DS field of a packet to a particular codepoint, adding the marked packet to a particular DS behavior aggregate. Shapers delay some or all of the packets in a traffic stream in order to bring the stream into compliance with a traffic profile. A shaper usually has a finite-size buffer, and packets may be discarded if there is not sufficient buffer space to hold the delayed packets. Droppers discard some or all of the packets in a traffic stream in order to bring the stream into compliance with a traffic profile. This process is known as "policing" the stream. Note that a dropper can be implemented as a special case of a shaper by setting the shaper buffer size to zero (or a few) packets.

Ingress or egress nodes at the boundary of DS-domain are responsible for classification, marking, policing and shaping, and enforcing PHB of traffic classes. Nodes within the DS domain are responsible for buffer management and packet scheduling, i.e., enforce PHB.

The implementation of PHB is not standardized. RFC 2474 describes that PHBs might be implemented by several mechanisms, including strict priority queueing, weighted fair queueing, weighted round-robin, class based queueing, in isolation or in combination. [13] and [14] provide guidelines to implement these PHBs with different queuing disciplines in Linux and Cisco implementations, respectively.

It is interesting to examine the different DiffServ-related QoS mechanisms in MPLS, which is summarized in [15]. An important task in network design is to determine a target utilization level of network links. The selected utilization level depends on target QoS guarantees, failure handling policies, risk tolerance etc. The selected utilization level can be enforced in different ways

- No QoS, aggregate capacity planning: link capacity is adjusted to *expected* link load. Given a network topology, and the traffic matrix between the edge nodes, an uncapacitated network dimensioning problem must be solved for shortest path allocation. Often it is a constraint to find non-bifurcating paths.
- MPLS Traffic Engineering (TE): Link load is adjusted to *actual* link capacity. MPLS TE supports constraint-based routing, i.e, before selecting and reserving a label-switched path (LSP) in the MPLS domain, the ingress MPLS node examines, whether there are enough resources in the hops on the path. It executes constrained shortest path finding (CSPF) algorithm. ISIS and OSPF TE extensions aid to advertise actual link attributes.
- MPLS DiffServ: behavior aggregates or traffic classes are defined. Class capacities are adjusted to *expected* class load. There is a per-class capacity planning.
- MPLS DS-TE: class load is adjusted to *actual* class load. MPLS DS-TE brings per-class dimension to constrained based routing and per-class admission control. ISIS and OSPF TE extensions advertise per-class remaining

2.2.5.4 Concluding remarks for the QoS provisioning capabilities of OpenFlow switches

Current OF and OFconfig specifications recommend the support of HTB and HSCF queueing disciplines. The APIs are only able to create a one-level traffic class hierarchy instead of multiple level hierarchy applying a mixture of queueing disciplines, which would be needed to implement standard PHBs.

It can be seen from the QoS solutions for MPLS that for strong differentiation and fine optimization, the actual load of service classes must be measured and the decision logic must be informed about the actual or remaining class capacities and link capacities.

Another option is that capacities for service classes are provided based on expected traffic, hence min-rates, max-rates and other queueing discipline parameters could be set by network management.

In an SDN domain, per-class TE advertising functionality of OSPF or ISIS might not be needed, if the OpenFlow switches inform the controller about available bandwidth.

2.2.6 Related work concerning internet service quality assessment and automatic reaction

The standardization of mobile networks inherently addresses the topic of Quality of Service (QoS) and the respective service flow handling. The 3GPP defined architecture is called Policy and Charging Control (PCC) architecture, which started in Release 7 and applies now to the Evolved Packet System (EPS) [165]. QoS services and policy control of 3GPP architecture are summarized in Appendix A.

The Policy and Charging Rules Function (PCRF) is being informed about service specific QoS demands by the Application Function (AF). Together with the Traffic Detection Function (TDF) or the optionally available PCRF intrinsic Application Detection and Control (ADC), traffic flow start and end events are detected and indicated to the PCRF. This in turn checks the Subscription Profile Repository (SPR) or the User Data Repository (UDR) for the permission of actions as well as the Bearer Binding and Event Reporting Function (BBERF) for the current state of already established dedicated bearers. As can be seen here, the 3GPP QoS control relies on the setup of QoS by reserving dedicated bearers. These bearers need to be setup, torn down for service flows or modified in their resource reservation, if several flows are being bundled into the same bearer [166]. Nine QoS Class IDs (QCI) have been defined by 3GPP for LTE networks, which are associated with such dedicated bearers. Today, IP Multimedia Subsystem (IMS) based external services and or provider own services make use of this well-defined PCC architecture and setup dedicated service flow specific reservations by means of those bearers. Ordinary Internet services, however, are often carried in just one (default) bearer without any reservations and thus experience considerable quality degradations for streaming and real time services. Therefore, network operators need to address and differentiate service flows besides the standardized QoS mechanisms of the 3GPP. HTTP based adaptive streaming video applications currently amount the highest traffic share (see [164]). They need to be investigated for their application behaviour and appropriate actions should be incorporated in any QoS enhancing framework architecture. An overview of HTTP based streaming services can be found in [167]. There are many approaches found in the literature, which address specific services and potential enhancements. HTTP Adaptive Streaming Services (HAS) [168] for instance is a new way to adapt the video streaming quality based on the observed transport quality. Other approaches target the increasing trend of Fixed-Mobile Convergence (FMC) and network sharing concepts, which inherently require the interlinking of PCRF and QoS architecture structures and mechanisms (see e.g. [169]). This architectural opening is particularly interesting for the interlinking of 3GPP and non-3GPP QoS concepts, but has not yet been standardized for close QoS interworking. The proposed interworking of WiMAX and LTE networks [170] and the Session Initiation Protocol (SIP) based Next Generation Network (NGN) QoE Controller concept [171] are just examples of the recent activities in the field. The ISAAR framework presented in this paper follows a different approach. It aims for service flow differentiation either within single bearers without PCRF support or PCRF based flow treatment triggering dedicated bearer setups using the Rx interface. This way it is possible to use ISAAR as a standalone solution as well as aligned with the 3GPP PCRF support.

2.3 Mobility management

This section discusses the state-of-the-art of mobility management, including existing IP mobility management solutions. Main characteristics of mobility management schemes are the following:

- centralized, distributed user and control plane, or partially distributed when only the user plane is distributed, but not the control plane,
- static (always on, also when there is no need for IP mobility management) or dynamic (on-demand/need),
- supported mobility types: terminal, network, flow, session mobility.

We also present state-of-the-art of introduction of virtualization techniques into existing mobile network architectures, and particularly the influence of virtualization on the mobility management. Finally, we discuss separately a HIP-based mobility management scheme, which is a secure, partially distributed mobility management solution for HIP-aware mobile nodes.

2.3.1 Definition of mobility management

Mobility is one of the most unique characteristics of future's convergent architectures but this promising feature also introduces a whole bunch of new challenges to the original Internet. Mobility protocols are needed to allow mobile terminals to change their Internet points of attachment while continuously maintaining reachability and ongoing communication sessions in the widest range of different scenarios and types of mobility. In order to achieve this, location information of moving devices must be stored and updated in the network. However, such support was not included as a feature in the original TCP/IP protocol stack because the legacy Internet was designed for fixed devices; mobility features were added later to the IP infrastructure.

When considering mobility management, at least two main types of mobility should be classified. On one hand single mobile nodes have to be taken into account (i.e. host or terminal mobility). This kind of mobility allows a node to maintain ongoing communication or commence/receive incoming session requests independently from its network point of attachment. On the other hand, mobility should not be limited to single moving terminals: data communications within entire mobile networks moving between different access points need to be managed as single entities (i.e. network mobility). This kind of mobility requires at least one central entity in a moving network in order to hide the inside operation.

The emerging wireless technologies introduced several other types of mobility. We can talk about device-centric, low-level mobility including ad hoc mobility (mobile nodes are reachable and routable in ad hoc structures) and mode mobility (nodes can interchange between ad hoc and infrastructure modes). There is a high level user-centric mobility consisting of personal mobility (e.g., one address for many different terminals), session mobility (communication sessions are interchangeable between devices) and service mobility (services are maintained during the movements).

The appearance of heterogeneous networking and multi-access devices introduced another classification: managing mobility between different types of access networks (e.g., UMTS to Wi-Fi) is called "vertical handover", while "horizontal handover" is the case of mobility between homogeneous networks (e.g., when a UE leaves a cell and enters another one in a 3G network). (Please note that the definition of horizontal and vertical handover is little bit vague. E.g., a handover from a 802.11g WLAN link towards an 802.11b link can be considered as either a vertical or a horizontal handover, depending on the point of view.)

However, one thing is surely the same either talking about host or network, vertical or horizontal, or any other kind of mobility: wireless networks cover a definite geographical area consisting of several different domains. Deriving from this, mobile nodes can change their point of attachment to the network basically in two different ways. In the first case users can move inside a single domain, which is usually referred as intra-domain mobility. In the second case users can roam between different domains, which case is called inter-domain mobility. Usually, domains are aggregated and a special protocol is responsible for the local mobility management of this group of domains in order to offer fast and seamless handover control over a limited geographical area. In such cases, we speak about micromobility, and the aggregated group of domains is called micromobility domain. Micromobility protocols are designed for environments where mobile terminals change their network point of attachment so often that the general mobility management protocols (i.e. macromobility solutions) originate excrescent overhead and ineffective operation.

When multiple access technologies are simultaneously available for using Internet resources, the user can dynamically change between them. This is the so-called multihoming. However, using such situation raises the problem of how packets should be distributed among available interfaces. If the user runs several applications with several flows, each flow has its own criteria which usually contradict each other. Multihoming and mobility can be controlled on the terminal/host level (this is called per-host, or per-terminal mobility), but also the connection of each communication flow is handled independently (this is called per-flow or per-application mobility).

Expected huge data traffic growth creates scalability requirements that might lead to more distributed network architecture. Distributed and flat mobile networks not only require novel architectural design paradigms, special network nodes and proprietary elements with peculiar functions, but also require certain, distinctive mobility management schemes sufficiently adapted to the flat way of operation by being distributed in nature. In fact such distributed mobility management mechanisms (DMM) and the relating methods form the key routines of the future mobile Internet designs.

2.3.2 Introduction to virtualization in technologies supporting mobile broadband networks / mobile services

LTE/EPC is a fit-for-purpose closed architecture based on 3GPP-standardized interfaces, where every functional block and entity performs a specific set of functions, and each of the interfaces likely runs a unique protocol and owns a unique definition. Evolution of mobile broadband networks within such a strictly bound framework has several barriers. On one hand, operators have to struggle with higher CAPEX/OPEX expenditures in an age when average revenue per user is continuously decreasing. On the other hand, the high level of specialization of each EPC building block (all of them strictly defined to operate in and only in EPC architectures), has seriously limited the flexibility and openness. These HW/SW elements very rarely can be extended using open interfaces or APIs: if an operator wants to implement new kinds of network services to its users, existing equipment will not provide much help when developing and deploying such services.

After recognizing the above issues, telecommunication system operators started to re-build their networks by eliminating specialized hardware elements, or proprietary boxes and interfaces. After several years of practical experience with heterogeneous pools of generalized hardware components, middleware architectures, application and service provisioning frameworks, wireless and mobile operators are fully aware of pros (high level of infrastructure centralization, control the environment, keeping evrithing patched and maintained, automating activities, cost efficiency, etc.) and cons (technical difficulties, security issues, cooling and ventilation, etc.) of managing large-scale computing and storage infrastructures. This drives the expectation that mobile network operators will increasingly adopt virtualization[2], softwarization[3] and cloudification[4] based approaches within their infrastructures in order to streamline their operations, control CAPEX/OPEX, optimize handling of user traffic, and address the challenges.

2.3.3 Mobility Management State of the Art Technologies

This section introduces the needs for evolving actual mobile networks and the applied mobility management techniques towards a more distributed solution, eventually being able to operate in virtualized environments.

2.3.3.1 Distributed Mobility Management

Novel design paradigms of mobile networks not only need innovation in the architecture in the form of functional distribution, softwarization, virtualization and cloudification, but also demand certain, distinctive mobility management schemes sufficiently adapted to the novel architecture. The importance of this research area was firstly discovered by the creation of a new IETF non-working group called Distributed Mobility Management (DMM) [55] [54] in August 2010, forming a fully operating working group a year after aiming to extend IP mobility solutions for more scalable networking architectures of distributed, flat and ultra flat network designs. These technologies can be considered as the predecessor technologies for SDMNs.

Mobility management solutions nowadays rely on hierarchical and centralized architectures, which employ anchor nodes for mobility signaling and user traffic forwarding. In 3G UMTS architectures centralized and hierarchical mobility anchors are implemented by the RNC, SGSN and GGSN nodes that handle traffic forwarding tasks using the apparatus of GPRS Tunneling Protocol (GTP). The similar centralization is noticeable in Mobile IP (MIP) [23] where the Home Agent –an anchor node for both signaling and user plane traffic– administers mobile terminals' location information, and tunnels user traffic towards the mobile's current locations and vice versa. Several enhancements and extensions such as Fast Handoffs for Mobile IPv6 (FMIP) [24], Hierarchical Mobile IPv6 (HMIP) [25], Multiple Care-of Addresses (MCoA) Registration [26], Network Mobility (NEMO) Basic Support [27], Dual-Stack Mobile IPv6 [28], and Proxy Mobile IPv6 (PMIPv6) [29], were proposed to optimize the performance and broaden the capabilities of

[2] Creating a virtual version of some networking or computing resource

[3] Mature and highly integrated programmability at all levels of the infrstructure

[4] Trend of programs having migrated from local installations to remote resources requiring online connection at all times

Mobile IP, but all of them preserve the centralized and anchoring nature of the original scheme (please see Figure 16 and Figure 17 for details of MIPv6, NEMO/MCoA and PMIPv6).

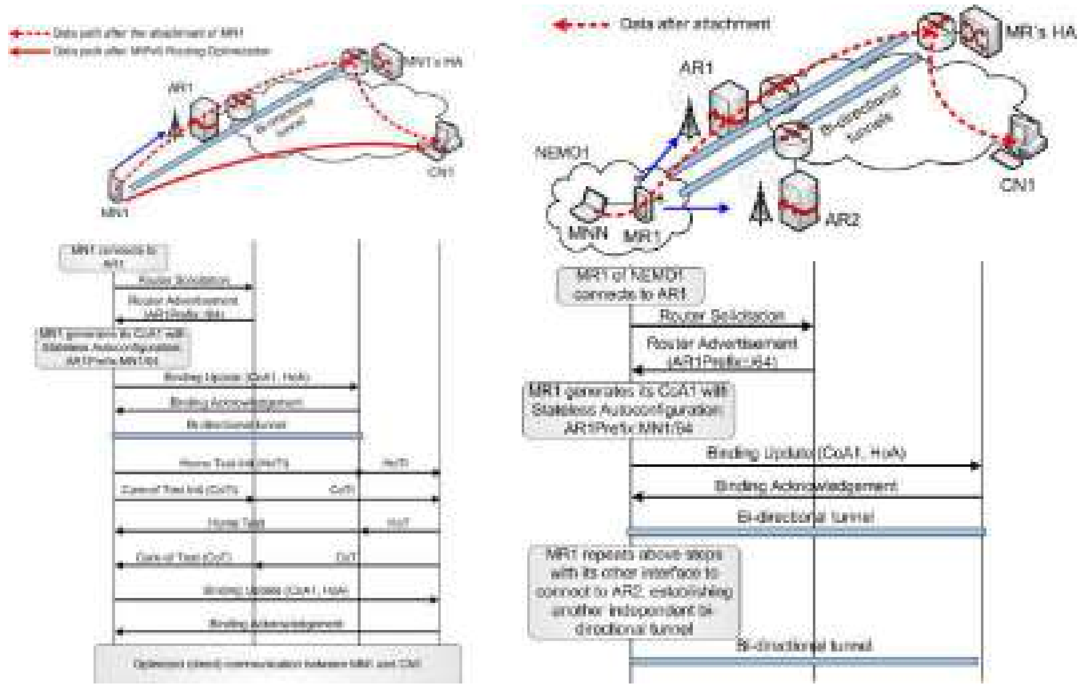
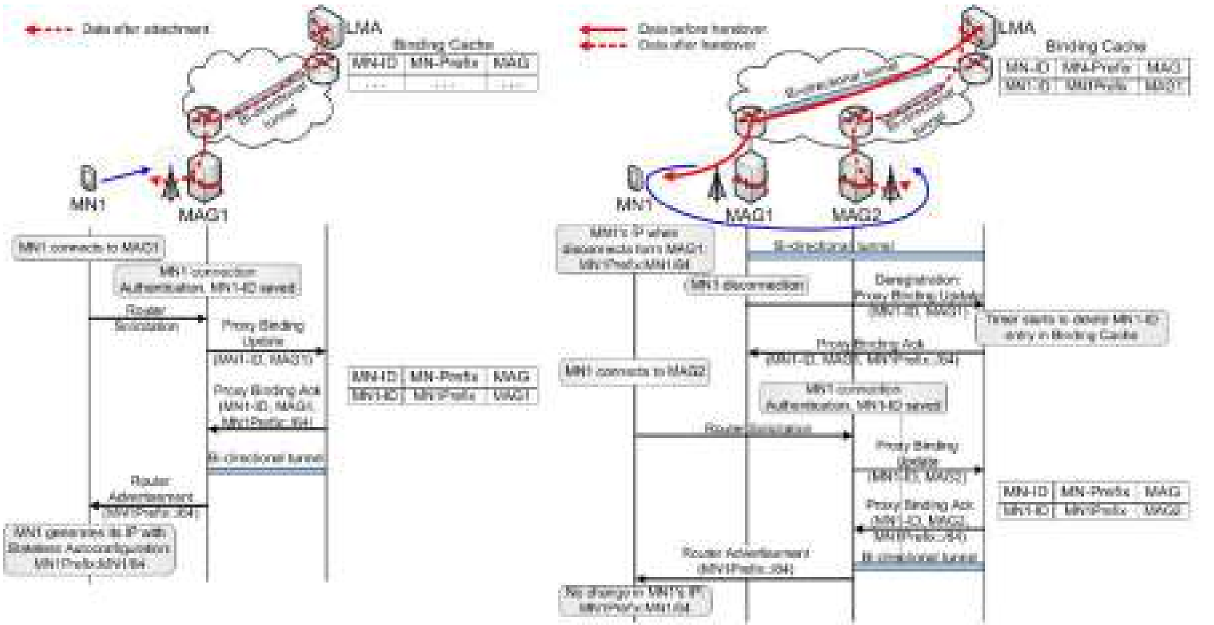

Data path after the attachment of MN1
Data path after MIPv6 Routing Optimization
MN1's HA
AR1
Bi-directional tunnel
CN1
MN1
MN1 connects to AR1
Router Solicitation
Router Advertisement (AR1Prefix::/64)
MN1 generates its CoA1 with Stateless Autoconfiguration AR1Prefix:MN1/64
Binding Update (CoA1, HoA)
Binding Acknowledgement
Bi-directional tunnel
Home Test Init (HoTI)
HoTI
Care-of Test Init (CoTI)
CoTI
Home Test
HoT
Care-of Test (CoT)
CoT
Binding Update (CoA1, HoA)
Binding Acknowledgement
Optimized (direct) communication between MN1 and CN1
Data after attachment
MR's HA
AR1
NEMO1
Bi-directional tunnels
CN1
MNN
MR1
AR2
MR1 of NEMO1 connects to AR1
Router Solicitation
Router Advertisement (AR1Prefix::/64)
MR1 generates its CoA1 with Stateless Autoconfiguration AR1Prefix:MN1/64
Binding Update (CoA1, HoA)
Binding Acknowledgement
Bi-directional tunnel
MR1 repeats above steps with its other interface to connect to AR2, establishing another independent bi-directional tunnel
Bi-directional tunnel

Figure 16 – MIPv6 and NEMO MCoA architecture and operation [72].

There are also alternate schemes in the literature aiming to integrate IP-based mobility protocols into cellular architectures and to effectively manage heterogeneous networks with special mobility scenarios. Cellular IP [30] introduces a gateway router dealing with local mobility management while also supporting a number of handoff techniques and paging. A similar approach is the handoff-aware wireless access Internet infrastructure (HAWAII) [31], which is a separate routing protocol to handle micromobility. Terminal Independent Mobility for IP [32] combines some advantages from Cellular IP and HAWAII, where terminals with legacy IP stacks have the same degree of mobility as terminals with mobility-aware IP stacks. Authors of [33] present a framework that integrates 802.21 Media Independent Handover [34] and Mobile IP for network driven mobility. A similar framework is the Access Network Discovery and Selection Function (ANDSF) specified in 3GPP TS 23.261 [38] and 23.402 [39] for EPS. However, these proposals are also based on centralized functions and generally rely on MIP or similar anchoring schemes.


Data after attachment
LMA
Binding Cache
MN-ID
MN-Prefix
MAG
Bi-directional tunnel
MN1
MAG1
MN1 connects to MAG1
MN1 connection Authentication, MN1-ID saved
Router Solicitation
Proxy Binding Update (MN1-ID, MAG1)
MN1-ID
MN1Prefix
MAG1
Proxy Binding Ack (MN1-ID, MAG1, MN1Prefix::/64)
Bi-directional tunnel
Router Advertisement (MN1Prefix::/64)
MN1 generates its IP with Stateless Autoconfiguration MN1Prefix:MN1/64
Data before handover
Data after handover
LMA
Binding Cache
MN-ID
MN-Prefix
MAG
MN1-ID
MN1Prefix
MAG1
Bi-directional tunnel
MN1
MAG1
MAG2
MN1's IP when disconnects form MAG1: MN1Prefix:MN1/64
Bi-directional tunnel
MN1 disconnection
Deregistration: Proxy Binding Update (MN1-ID, MAG1)
Timer starts to delete MN1-ID entry in Binding Cache
Proxy Binding Ack (MN1-ID, MAG1, MN1Prefix::/64)
MN1 connects to MAG2
MN1 connection Authentication, MN1-ID saved
Router Solicitation
Proxy Binding Update (MN1-ID, MAG2)
MN-ID
MN-Prefix
MAG
MN1-ID
MN1Prefix
MAG2
Proxy Binding Ack (MN1-ID, MAG2, MN1Prefix::/64)
Router Advertisement (MN1Prefix::/64)
Bi-directional tunnel
No change in MN1's IP: MN1Prefix:MN1/64

a) MN1 attaches to the PMIPv6 domain

b) MN1 handover between MAG1 and MAG2 inside PMIPv6 domain

Figure 17 - PMIPv6 environment and signalling framework [72].

Some of the above solutions are already standardized [35] [36] [37] for 3G and beyond 3G architectures where the introduced architectural evolution is in progress: E-UTRAN (Evolved Universal Terrestrial Radio Access Network) or LTE (Long Term Evolution) base stations (eNodeBs) became distributed in a flatter scheme allowing almost complete distribution of radio and handover control mechanisms together with direct logical interfaces for inter-eNodeB communications. Here, traffic forwarding between neighboring eNodeBs is temporarily allowed during handover events providing intra-domain mobility. However, traffic forwarding and inter-gateway mobility operations remain centralized thanks to S-GW, PDN-GW, Local Mobility Anchor and Home Agent, responsible for maintaining and switching centralized, hierarchical and overlapping system of tunnels towards mobile nodes. Also, offloading with Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) extensions [40] [41] cannot completely solve this issue: mobility management mechanisms in current wireless and mobile networks anchor the user traffic relatively far from users' location and make it hard to eliminate the centralized network build-up. This results in unscalable data plane and control plane with non-optimal routes, overhead and high end-to-end packet delay even in case of motionless users, centralized context maintenance, single point of failures, and no natural possibilities for virtualization. Anchor-based traffic forwarding and mobility management solutions also cause deployment issues for caching contents near the user, and for software define networking.

To solve all the problems and questions like non-optimal routes, non-optimality in evolved architectures, low scalability of centralized routing and context management, single point of failures, mobility signaling overhead and wasting resources to support mobile nodes not needing mobility support [73], novel mobility management approaches must be envisaged, applicable to intra- and inter-technology mobility cases as well.

2.3.3.1.1 Main scenarios of distributed mobility management (DMM)

The basic idea is that anchor nodes and mobility management functions of wireless and mobile systems could be distributed to multiple locations in different network segments, hence mobile nodes located in any of these locations could be served by a close entity (Figure 18).

A first alternative for achieving DMM is core-level distribution. In this case mobility anchors are topologically distributed and cover specific geographical area but still remain in the core network. A good example is the Global HA to HA protocol [42], which extends MIP and NEMO in order to remove their link layer dependencies on the Home Link and distribute the Home Agents in Layer 3, at the scale of the Internet. DIMA (Distributed IP Mobility Approach) [43] can also be considered as a core-level scheme by allowing the distribution of MIP Home Agent (the normally isolated central server) to many and less powerful interworking servers called Mobility Agents (MA). These new nodes have the combined functionality of a MIP Home Agent and HMIP/PMIP Mobility Anchor Points. The administration of the system of distributed MAs is done via a distributed Home Agent overlay table structure based on a Distributed Hash Table (DHT) [44]. It creates a virtual Home Agent cluster with distributed binding cache that maps a mobile node's permanent identifier to its temporary identifier.

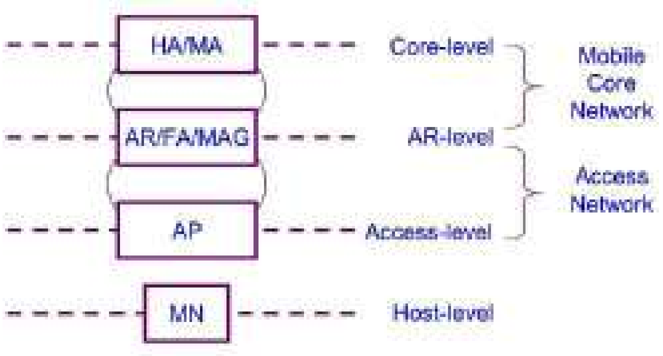


Figure 18 – Different levels of functional distribution in DMM schemes [73].

A second alternative for DMM is when mobility functions and anchors are distributed in the access part of the network. For example in case of pico- and femto cellular access schemes it could be very effective to introduce Layer 3 capability in access nodes to handle IP mobility management and to provide higher level intervention and even cross-layer optimization mechanisms. The concept of UMTS Base Station Router (BSR) [45] realizes such an access-level mobility management distribution scheme where a special network element called BSR is used to build flat cellular systems. BSR merges the GGSN, SGSN, RNC and NodeB entities into a single element: while a common UMTS network is built from a plethora of network nodes and is maintained in a hierarchical and centralized fashion, the BSR integrates all radio access and core functions. Furthermore, the BSR can be considered a special wireless edge router that bridges between mobile/wireless and IP communication. In order to achieve this, mobility support in the BSR is handled at three layers: RF channel mobility, Layer 2 anchor mobility, and Layer 3 IP mobility. The idea of Liu Yu et al. [46] is quite similar to the BSR concept. Here a node called Access Gateway (AGW) is introduced to implement distributed mobility management functionalities at the access level. The whole flat architecture consists of two kinds of elements, AGW on the access network side and terminals on the user side. Core network nodes are mainly simple IP routers. The scheme applies DHT and Loc/ID separation: each mobile node has a unique identifier (ID) keeping persistent, and an IP address based locator (Loc) changed by every single mobility event. The (Loc,ID) pair of each mobile is stored inside AGW nodes and organized/managed using DHTs. [74] also proposes an access-level solution by moving the HA functions to the edge of the network, being deployed into the gateway router into the access routers called Distributed Anchor Routers (DARs). This scheme (Figure 19) also introduces dynamicity into the mobility management. In cases when the MN wants to keep the reachability of one or more IP addresses it obtained from a previous DAR, the MN has to involve its MIPv6 protocol stack by sending a Binding Update to the DAR where the IPv6 address is anchored using the address obtained from the current DAR as care-of-address. If the provision of session continuity is not needed, the MIPv6-based operation will just skipped. Note that this decision is dynamic and can be done even on an application basis (i.e., the system will deal with handovers for a VoIP application, but will skip this operation for HTTP web browsing).

A third type of DMM application scenarios is the so-called host-level or peer-to-peer distributed mobility management where once the correspondent node is found, communicating peers can directly exchange IP packets. In order to find the correspondent node, a special information server is required in the network, which can also be centralized or distributed. A good example for host-level schemes in the IP layer is MIPv6 which is able to bypass the user plane anchor (i.e., Home Agent) due to its route optimization mechanism, therefore providing a host-to-host communication method. End-to-end mobility management protocols working in higher layers of the TCP/IP stack such as Host Identity Protocol (HIP) [47] [47], TCP-Migrate [48], MSOCKS [49], Stream Control Transmission Protocol (SCTP) [50], or Session Initiation Protocol (SIP) [51] can also be efficiently employed in such schemes.

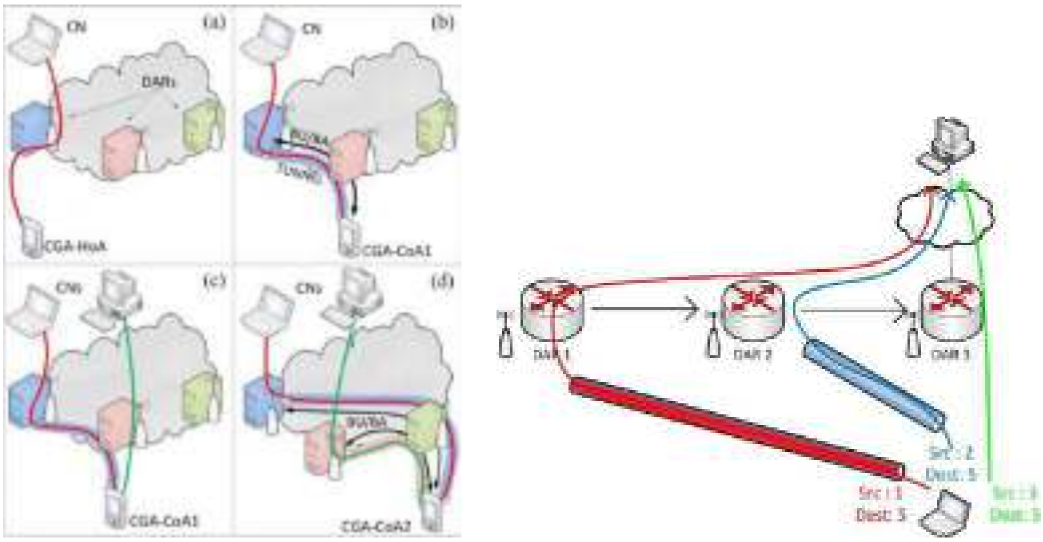


Figure 19 – A good example for access-level distribution of functions Flat Access and Mobility Architecture [74].

2.3.3.1.2 Methods for distribution of mobility functions

Mobility management functions can be distributed in two main ways: partially and fully.

Partially distributed schemes can be implemented either by distinguishing signaling and user planes based on their differences in traffic volume or end-host behavior (i.e., only the user plane is distributed), or by granting mobility support only to nodes that actually need it (i.e., actually eventuate mobility event), hence achieving more advanced resource management. Note that these two approaches may also be combined.

Today's mobility management protocols (e.g., Mobile IP, NEMO BS and Proxy Mobile IP without route optimization) do not separate signaling and user planes which means that all control and data packets traverse the centralized or hierarchized mobility anchor. Since the volume of user plane traffic is much higher compared to the signaling traffic, the separation of signaling and user planes together with the distribution of the user plane but without eliminating signaling anchors can still result in effective and scalable mobility management. This is exploited by the HIP based UFA scheme [52] [53] where a relatively simple inter-UFA GW protocol can be used thanks to the centralized HIP signaling plane, but the user plane is still fully distributed. Mobile IP based DMM solutions also rely on the advantages of this partial distribution concept when they implement route optimization, hence separate control packets from data messages after a short period of route optimization procedure.

The second type of partially distributed mobility management is based on the capability to turn off mobility signaling when such mechanisms are not needed. This so-called dynamic mobility management dynamically executes mobility functions only for mobile nodes that are actually subjected to handover event, and lack transport or application-layer mobility support. In such cases, thanks to the removal of unwanted mobility signaling, handover latency and control overhead can be significantly reduced. Integrating this concept with distributed anchors, the algorithms supporting dynamic mobility could also be distributed. Such integration is accomplished in [54] [55] where authors introduce and evaluate a scheme to dynamically anchor mobile nodes' traffic in distributed Access Nodes (AN), depending on mobiles' actual location when sessions are getting set up. The solution's dynamic nature lies in the fact that sessions of mobile nodes are dynamically anchored on different ANs depending on the IP address used. Based on this behavior, the system is able to avoid execution of mobility management functions (e.g., traffic encapsulation) as long as a particular mobile node is not moving. The method is simultaneously dynamic and distributed, and because mobility functions are fully managed at the access level (by the ANs), it is appropriate for flat architectures. Similar considerations are applied in [56] for MIP, in [57] for HMIP and in [58] for PMIP. The MIP-based scheme introduces a special mode for the mobility usage in IP networks: for all the IP sessions opened and closed in the same IP sub-network no MIP functions will be executed even if the mobile node is away from its home network; standard MIP mechanisms will be used only for the ongoing communications while the mobile node is in motion between different IP sub-networks. The HMIP-based method proposes a strategy to evenly distribute the signaling burden and to dynamically adjust the micromobility domain (i.e., regional network) boundary according to real-time measurements of handover rates or traffic load in the networks. The PMIP-based solution discusses a possible deployment scheme of Proxy Mobile IP for flat architecture. This extension allows to dynamically distributing mobility functions among access routers: the mobility support is restricted to the access level, and adapted dynamically to the needs of mobile nodes by applying traffic redirection only to MNs' flows when an IP handover event occurs.

Fully distributed schemes bring complete distribution of mobility functions into effect (i.e., both data plane and control plane are distributed). This implies the introduction of special mechanisms in order to identify the anchor that manages mobility signaling and data forwarding of a particular mobile node, and in most cases this also requires the absolute distribution of mobility context database (e.g., for binding information) between every element of the distributed anchor system. Distributed Hash Table or anycast/broadcast/multicast communication can be used for the above purposes. In such schemes, usually all routing and signaling functions of mobility anchor nodes are integrated on the access level (like in [59]), but less flat architectures (e.g., by using Hi3 [60] for core-level distribution of HIP signaling plane) are also feasible.

2.3.3.2 SDN based mobility management techniques

Future mobile Internet architectures will become even more heterogeneous then today by interconnecting millions of users and applications over access networks ranging from wired, infrastructure-based wireless (e.g., cellular-based networks, V2I networks, wireless mesh networks), to infrastructure-less wireless networks (e.g., mobile ad-hoc networks, V2V networks). As mobile end terminals with multiple network interfaces become widespread, users will demand high quality service regardless of location, time, or type of Internet access. Self-organizing networks are envisioned to extend the range of infrastructure-based access, or handle connectivity problems. Self-organizing networks may thus enable a variety of new applications such as cloud-based services, cooperative vehicular communication, eHealth and mHealth applications, emergency response, etc. Efficient content delivery over mobile and wireless access networks will become essential functions very soon, therefore self-organizing networks easily could become a crucial part of the future mobile Internet.

The SDN/SDMN paradigm has the potential to facilitate and ease the deployment and continuous maintenance of network applications and services with great efficiency and flexibility. While there are existing previous work focusing on SDN usage in wireless and mobile environments, the scope has primarily focused on infrastructure-based deployments (e.g., Wi-Fi access points). An important example is the OpenRoads project [75], in which authors envisioned a world where users are able to freely move between wireless access networks. The OpenRoads architecture consists of three different layers: flow, slicing and controller. These layers implement flexible control, virtualization and abstraction in order to provide a framework where researches are able to implement different mobility management algorithms and run them concurrently in the software defined networking infrastructure. OpenRoads also incorporates multiple wireless technologies (e.g., WiMAX and Wi-Fi).

A recent publication [78] introduces a blueprint for implementing current as well as future network architectures based on a software-defined networking approach. The architecture is called MobileFlow and enables operators to capitalize on a flow-based forwarding model and fosters a rich environment for innovation inside the mobile network.

Authors of [79] proposed an OpenFlow based real-time media delivery platform in order to provide high performance and reliability for video streaming in heterogeneous networking architectures. The scheme allows mobile terminals to be connected to several APs simultaneously and to switch fast between them with the help of the SDN flow switching technology (see Figure 20 for details). Other existing works like such as [76] [77] have examined OpenFlow in environments incorporating wireless mesh networks.

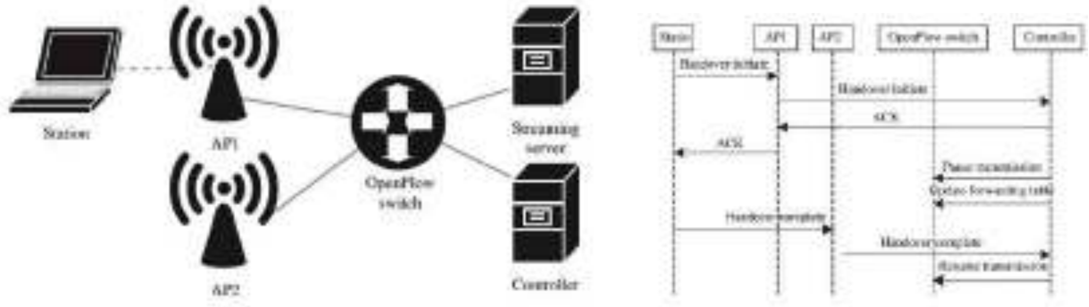


Figure 20 – An SDN based handover framework for real-time media delivery [79].

2.3.4 Existing mobility management proposals for SDMNs

Mobility management tasks and different mobility scenarios introduced in Section 2.3.1 are still relevant in the 3GPP introduced Evolved Packet Core (EPC) that is an all-IP mobile telecommunication architecture for LTE and LTE-A. EPC for LTE services is currently under deployment by the operators aiming it tackle the problem caused by the ever-growing mobile internet traffic in the user plane. Motivated by the strong need of scalability, various techniques to offload mobile traffic were developed and standardized like the already mentioned LIPA, SIPTO, DMM solutions and distributed/flat/ultra flat architecture alternatives. Similarly, the scalability problems of the control plane have also emerged. An important question within the above introduced problem space is how to decouple the control- and user- planes of mobility management used in EPC: if this decoupling is efficient, virtualization-enabled mobile and wireless infrastructures can be easily designed and deployed by satisfying the need of interoperability support across multiple vendors and hardware/software platforms. Otherwise, fragmentation of virtualization efforts will happen due to many separated protocols in proprietary solutions. The MIPv6 protocol family standardized by IETF, and the similar technique of GPRS Tunneling Protocol (GTP) by 3GPP establish a data path for a mobile node between the mobile node and its anchor point/points. Independently from the fact whether the tunnel is terminated inside the network (e.g., PMIPv6 [63]) or on the mobile terminal (MIPv6 [23]/DSMIPv6 [64]), the control and the user planes of these mobility protocols are tightly related and cannot be decoupled. (Note, that control plane is used for location update handover signaling and for establishing secure connections, while data plane is used for data transmission from the corresponding nodes (CN) to MNs and vice versa.) Control and data plane separation is defined also as a requirement for DMM. The solution of [65] is a good example for separation of control and user planes in mobility management, while [69] further extends the original idea for enhanced applicability in cloud-like infrastructures.

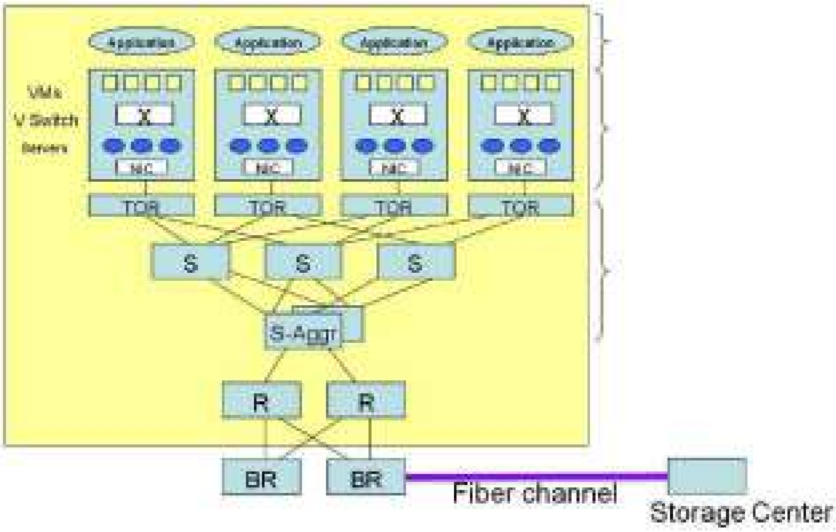


Figure 21 – General cloud networking structure [70].

Authors of [69] introduce a general architecture of cloud networking where the Top of Rack Switch (ToR) is a switch in a cloud architecture that is connected to the servers hosting virtual machines (Figure 21). A cloud network has one or more Data Center Border Routers (BR) or edge routers that connect the cloud to the Internet including other cloud networks or storage networks. Upon this general structure, [69] proposes to separate MIPv6 control and data plane by dividing HA into two functional entities: control plane functional entity and data plane functional entity (Figure 22). These entities can be placed and hosted on different physical elements, but must share a common database containing the Binding Cache and the security association information (e.g., IPSec keys). Home Agent Data Plane function can be deployed as a virtual machine in the cloud infrastructure, while Binding Cache and security association information could be placed in the storage center of the same cloud infrastructure. Home Agent Control Plane function is geographically more distributed in nature than the Data Plane, therefore it is placed closer to the mobile nodes. MNs first communicate with the Control Plane function in order to create the security association, which is followed by the address configuration and binding registration duties. After these procedures the MN is able to send/receive data packets using the Data Plane functionality closest to the MN's actual internet point of attachment (i.e., the link MN is using). When a mobile moves, it performs the handover signaling by communicating with the Control Plane function, which updates the Binding Cache according to the new information. After these procedures, the Control plane function will be able to inform the new data plane function in the target link about the novel Binding Cache data, and then mobile node can start to receive/send data with the help of the new Data Plane function. For this operation the MN must keep the address of the HA Control Plane function in cache so that it can perform handover signaling with it. According to the proposal of [69] this HA Data Plane function address can be provided by HA the Control Plane function to MN in an Alternate Home Agent Tunnel Address option defined in [71] by means of a Binding Acknowledgement message. The mobile node starts tunneling data packets and sends them to Alternate Home Agent Tunnel Address, and also received data packets will be tunneled from the Alternate Home Agent Tunnel Address. The most important open question is how to share the Binding Cache and security associations database.

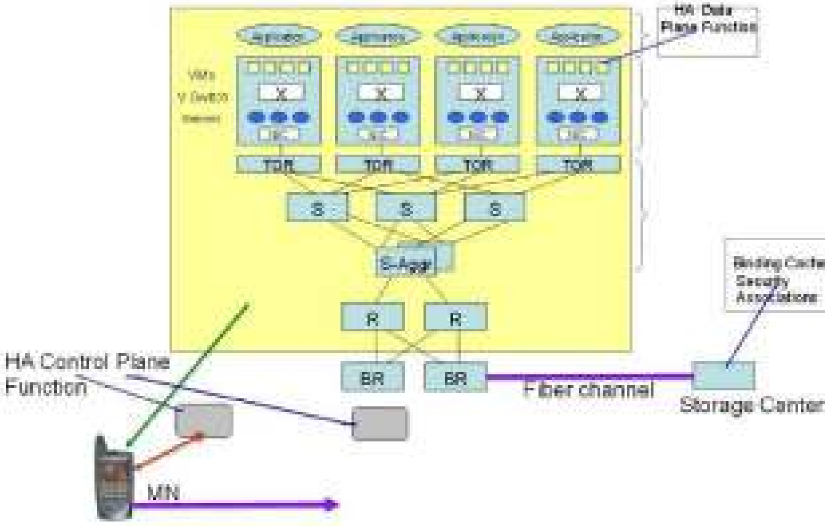


Figure 22 – MIPv6 use-case in a cloud-like mobile infrastructure [70].

There is another alternative of the latter solution if vEPC will be realized: we could have an opportunity to re-design the basic architecture of current mobility systems. Instead of tunneling packets like in today's solutions, we could just route the packets towards the mobile node and vice versa.

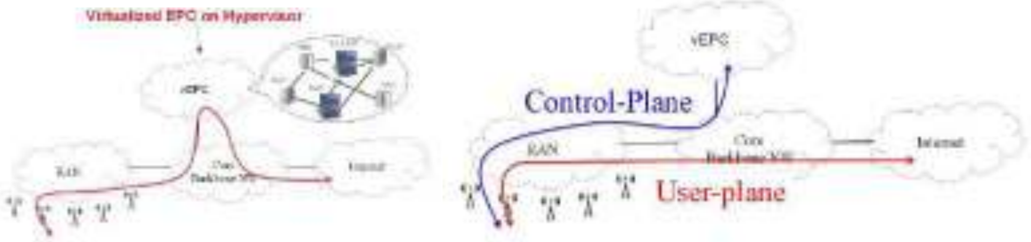


Figure 23 – Virtualized EPC architecture and splitting user-control plane functions [68].

Since a role of the user plane is esentially routing, routing protocols could be naturally used to forward UE's traffic. Authors of [62] propose a BGP-based solution, but Software Defined Networking (SDN) techniques – as introduced before – are also promising alternatives: Open Flow and other relevant protocols can setup the forward path dynamically according to UE's states available in the control plane (Figure 23). [62] does not forget that there were a good motivation for adapting tunneling in Mobile IP based solutions instead of pure IP routing, and that is global mobility provision: MNs should be reachable anywhere on the Internet. The routing-based global mobility solutions such as [66] and [67] have proved that it is feasible, but due to scalability and stability issues of the global network, this solution was not recommended by IETF. Despite the fact that global mobility is important, the reality is that cell phones are moving just within an operator's network fully controlled by the EPC architecture. If mobility events are limited within an operator, a routing based approach using multiple industry standard routers and switches could be a lot more feasible and practical compared to the solution of per-node tunnel path management in dedicated proprietary equipments like SGW and PGW. In the proposal of [62] switches and routers receive mobile nodes' forwarding information from the control plane of vEPC by the form of routing updates (Figure 24).

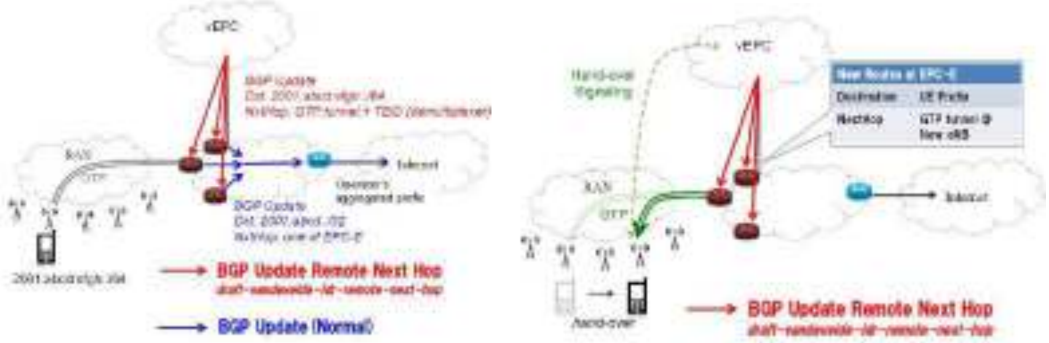


Figure 24 – Route update and Handover [68].

The introduced schemes and solutions are examples on possible mobility management approaches applicable in SDMNs. A more thorough survey of such existing techniques will be provided in the following deliverables, aiming to draw the missing points and exactly define SIGMONA research directions.

2.3.5 HIP-based mobility management using signaling delegation

Due to their centralized, modularly divisible design, mobile network architectures currently being under deployment would not scale particularly well to efficiently handle the increasing traffic. In centralized architecture, a specific gateway (GW) is in charge of allocating an IP address to the terminals and managing the context. Such context include mapping between customer profile, IP address, tunnel ID, bearer context. Tunnels are set up between terminals and centralized routers to transport IP traffic. IP routing and traffic management are made according to user's context and not only based on IP header. These require certain memory and CPU resources per user at the GW (and other centralized network elements). Scalability issue concerns the user and control plane of centralized network functions when the number of connected users and the bandwidth per user increase. Regarding centralized, modularly divisible network functions, depending on the speed of the data bandwidth increase, constraints for centralized equipments are CAPEX and OPEX proportional to traffic volume at busy hour and operational constraints to roll out new developments and to upgrade the network. Potential traffic anchors in 3GPP core network in the user plane are the GGSN, PDN GW, while potential control traffic anchors are e.g., the P-CSCF and MME. Reduction of signaling load related to establishment and handover procedures is hence one of the important challenges for mobile networks architectures.

As one of the concepts to enhance scalability of the core network, the Ultra Flat architecture (UFA) has been introduced by Daoud et al. [134]. UFA represents the ultimate step toward flattening the packet-switched domain of mobile networks. The objective of the UFA design is to distribute core network functions into single nodes at the edge of the network. Certain control functions could remain centralized, e.g., the subscriber information base, domain name resolution service and addressing service, which resolve application-level identifiers to the IP address of the peers. The intelligent nodes at the edge of the network are called UFA GWs. The user data traffic is conveyed directly between communicating parties through these GWs. GWs serve as breakout points toward content distribution networks and Internet services. In the proposal of Daoud et al. the functions of UFA control plane are realized using the Session Initiation Protocol (SIP). SIP-based UFA session establishment and mobility management procedures provide more efficient QoS services than in the existing 3GPP architectures and allow network-control, therefore greatly contribute to the reduction of resource consumption and increase the scalability.

Even though SIP is a very powerful signaling solution for UFA, it is not applicable for non-SIP (e.g., legacy Internet) applications required by the users. SIP-based control plane can not handle their mobility, authorization, accounting etc. Therefore, in [52][53] our main objective was to introduce a new alternative, i.e., Host Identity Protocol (HIP)-based signaling scheme for UFA, referred to as UFA HIP in the following. It must be noted that in [135], Daoud et al. proposed an SCTP-based extension for UFA to support SCTP-based communication.

Originally, HIP operates in an end-to-end or terminal-based fashion and provides authentication and key agreement, Internet Protocol security (IPsec) security association (SA) management and IP mobility management between pairs of endpoints. A network deploying the standard HIP control plane will be referred to as end-to-end HIP architecture (E-E HIP) in the following. The terminal-based control of E-E HIP has some drawbacks in an operator-controlled environment. The network has no ability to control and decrypt IPsec communication, which encumbers, e.g., traffic control, mobility management, adequate accounting, lawful interception by the operator. Additionally, a terminal-based control may cause unnecessary high network and computational overhead on the user equipments (UEs) and in the access networks, in an environment where radio resources are expensive.

UFA HIP introduces a hop-by-hop traffic forwarding approach, i.e., it divides the E-E SAs into two segments--one between the UE and the GW and the other between the GW and the peer of the UE. The split of SAs leads to the following problem during mobility of terminals in distributed networks. Inter-GW handovers result in session mobility for the HIP host associations (HAs) and IPsec SAs on the network-side between the source and target GW. Session mobility can be realized in two ways in different layers of the control plane: by context re-establishment at the target GW (i.e., in reactive way or proactively, such as pre-registration in 3GPP radios access networks [136] in the latter case) or by context transfers [139].

Context transfer-based solutions may facilitate fast handoffs, and reduce computational and network overhead and service-interruption time, hence are an attractive direction in the research of new signaling schemes for distributed mobile network architectures. Context-transfer in UFA HIP, however, is not as simple as conveying actual state information to a target GW. Regarding the concept of HIP, a HIP end-host can bind keying material, HIP HA, IPsec SA contexts only to its own (and the peer's) public/private key pairs in a cryptographic sense. Therefore, delegation of signaling right [140][141] becomes an important requirement in order to be able to create HIP and IPsec contexts in the name of the UE (with the UE's peers) by an intermediate GW. Session state transfer for other protocols is out of the scope of this work, but was addressed in several prior works, such as [137][138] regarding IPsec and IKEv2 state transfer, [142] describing transparent TCP connection passing or [143] for SIP context transfer between Proxy-Call Service Control Functions in IMS.

The delegation of signaling rights is also motivated by the optimization of resource utilization between the delegator and the delegate [140]. Delegates are temporarily authorized by the delegator to proceed in certain control tasks, such as periodic location updates, rekeyings, BEX, and notify the delegator about state changes. The delegator may issue a public-key authorization certificate to the delegate to proceed in his name at the peers. A delegator has the right to do so, because it updates or creates its own states stored at the remote peer. Public key authorization certificates contain the following information:

$$\{K^{+}_{\mathrm{delegator}}, K^{+}_{\mathrm{delegate}}, \mathrm{roles}, \mathrm{restrictions}\}_{K^{-}_{\mathrm{delegator}}}$$

where $K^{+}_{\mathrm{delegator}}$ and $K^{+}_{\mathrm{delegate}}$ and $K^{-}_{\mathrm{delegator}}$ denote the public key (HI) of the delegator and the delegate and the private key of the delegator, respectively. The private key is used to sign the certificate, and is never exposed to any party. If the restrictions enable the forwarding of the delegated roles to another delegate, then the delegate can further delegate the roles to another delegate forming certificate chains.

Herborn et al. [141] introduced HI delegation extension for HIP. Their proposal enables the movement of communication sessions between endpoint devices and transparent insertion and removal of intermediary routing or adaptation services. A delegate can use the HIT of the delegator and steer the traffic of correspondent nodes (CNs) to itself. However, in any case when HIP updates must be signed by the delegated HI, the delegate forwards the update messages to the delegator. The delegator signs with its private key and returns the updates to the delegates, which relay these messages to the CN. The main advantage of this approach is that it avoids the dissemination of private keys and allows temporary delegation of HIT. The delegation period is directly controlled by the delegator, since the delegator can cease the signing of the updates at any time for the delegate, and can any time rekey directly with the CN. Hence the delegator can keep track of state changes with CNs. The drawback is that if the private key owner disappears then the delegate may be forced to terminate the communication session when the next HIP update procedure is initiated, e.g., in case of rekeying or location update.

Another delegation technique is when shared keys are issued to a delegate, so it can generate Hashed-Message Authentication Codes (HMACs) admitted by the peer, as described in [144]. This solution leads to the complex and practically unfeasible problem of sharing secret keys with all possible CNs.

HIP is an enabler for advanced mobility management, supporting micromobility, network mobility, dual stack mobility, flow management, and location privacy [145]. Certain advanced mobility services require delegation of signaling rights of the UEs. E.g., when a UE changes micromobility domain then local RVS updates the global RVS in the name of the UE. In network mobility scenarios the HIP-enabled mobile routers are the delegates of mobile network nodes, which stay in the moving network. Mobile routers can update the CNs of UEs only if delegation is applied. We can see that in case of HI delegation, the latter scenario would cause the same amount of HIP signaling messages as if all mobile network nodes performed separately the location update procedures, due to the fact that the mobile router relays all updates through the mobile network nodes in order to get the public key signatures and to get accepted by their peers.

2.3.6 Overview of E-E and UFA HIP mobility management schemes

2.3.6.1 Overview of Host Identity Protocol

HIP operates in an E-E or terminal-based fashion and provides key agreement, Internet Protocol security (IPsec) security association (SA) management and IP mobility management between pairs of endpoints.

IPsec is a standardized protocol suite to provide encryption, integrity, message origin authentication and anti-replay protection for IP datagrams between two hosts. An SA is the bundle of algorithms and parameters on two hosts, being used to encrypt and authenticate IP datagrams selected by traffic selectors in one direction. For the protection of bi-directional traffic, an SA pair is required.

The initial SA establishment procedure is dubbed as Base Exchange (BEX) in HIP. After initial SA establishment there are forthcoming HIP update procedures for different purposes, such as rekeying, IP address update due to handovers, as described in Section 2.3.6.2.

HIP operates between the network and transport layer, and splits the identity and locator role of IP address. It means that the addressing is based on long-term, globally unique host identities (HIs) instead of short-term IP addresses. HIs are the public part from a public/private key pair associated uniquely with the HIP hosts. Host Identity Tag (HIT) is a 128-bit hash generated from the HI, having the same format as an IPv6 address. Legacy applications use the HIT for addressing peers. The HIP stack in the hosts is responsible for the translation of HITs to IP addresses and for the treatment of IP address changes and the presence of multiple network interfaces, seamlessly for the applications. HIP Host Association (HA) is a set of states in the control plane of peers established after a successful BEX. A HA includes the HIT and IP addresses of the peers, the key material, cipher suite for protection of the communication in the control plane, i.e., for protection of HIP communication, and user plane, that is, the parameters of the SA pair.

HIP-enabled hosts can register and keep updated their address at the rendezvous service (RVS). The purpose of RVS is the following. If the HIP stack of a host does not have up-to-date information on the locator of a peer, then the first HIP packet of BEX is sent toward the RVS and forwarded by the RVS to the actual locator of the destination peer. This is typically required for initial reachability of a peer or in case of simultaneous IP address change of the endpoints. If only one endpoint changes its address, then it notifies its peers with HIP update messages for the modification of the IP address in the existing HAs and SAs.

2.3.6.2 HIP BEX and update procedures

The BEX procedure is illustrated in Figure 25.

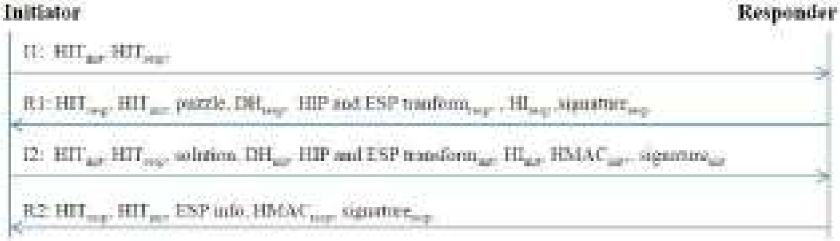

Initiator
Responder
I1: HIT_init, HIT_resp
R1: HIT_resp, HIT_init, puzzle, DH_resp, HIP and ESP tranform_resp, HI_resp, signature_resp
I2: HIT_init, HIT_resp, solution, DH_init, HIP and ESP transform_init, HI_init, HMAC_init, signature_init
R2: HIT_resp, HIT_init, ESP info, HMAC_resp, signature_resp

Figure 25 – HIP Base Exchange.

I1 packet starts the procedure, containing the HIT of the initiator and responder. I1 is a basic hello message and part of return routability procedure to check the availability of responder. R1 packet is a pre-created response to I1 packet.

The puzzle field in R1 contains a challenge for the initiator. In general, puzzle-based challenge-response mechanisms aim to mitigate denial-of-service attacks initiated from fake initiators against the responder. In HIP, the initiator must find a solution that, if given to a one-way hash function concatenated with this challenge, produces an output starting with a pre-defined number of. The expected number of zeros, i.e., difficulty level of the puzzle, is tunable by the responder. To find a good solution, the initiator must execute a brute-force search. The responder can verify the solution sent in I2 packet by only one hash function call. The responder does not establish HA and SA pair with the initiator until the reception of the good solution in I2.

The R1, I2 and R2 messages implement the standard authenticated Diffie-Hellman (DH) key exchange method [146]. The Hashed Message Authentication Codes (HMAC) provide message origin authenticity and integrity protection, and can be verified by the other peer knowing the integrity key. Public-key signatures provide authentication of the peer, the origin and integrity of the message, and can be checked by any peer using the HI of the signing entity as the public key. The Encapsulating Security Payload (ESP) info field contains the security parameter indexes, required for the identification of the SA pair.

Figure 26 presents the update procedure of HIP.

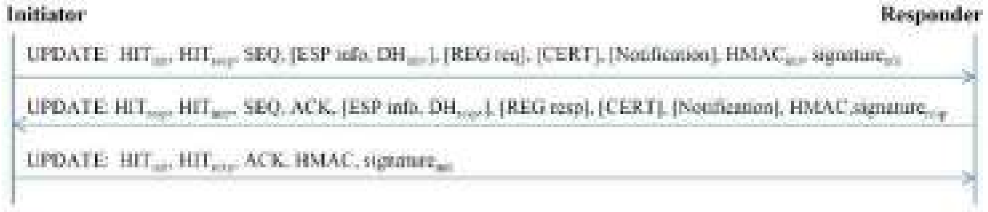

Initiator
Responder
UPDATE: HIT_{init}, HIT_{resp}, SEQ, [ESP info, DH_{init}], [REG req], [CERT], [Notification], $HMAC_{init}$, $signature_{init}$
UPDATE: HIT_{resp}, HIT_{init}, SEQ, ACK, [ESP info, DH_{resp}], [REG resp], [CERT], [Notification], HMAC signature$_{resp}$
UPDATE: HIT_{init}, HIT_{resp}, ACK, HMAC, $signature_{init}$

Figure 26 – HIP update.

The mandatory fields of an update packet are HITs, HMAC, signatures, the sequence and acknowledgment number. The latter two fields enable detection of packet loss and ordered delivery of update packets. Non-mandatory fields are the following. Notification carries control data, e.g., the new IP address of a mobile peer. DH public key values are sent in case of rekeying for calculation of a fresh DH secret and key material for the HA and the related SA pair. The registration request and response (REG req and resp) enable subscription to a service of the peer, such as delegation of signaling or RVS service. CERT field carries the certificate-chain, which proves that the signature is valid and the update procedure is authorized. An update procedure normally contains three packets. However, if the size of CERT field or a Notification field together with the other ones is larger than the maximum transfer unit size of the network then these fields are sent in multiple packets to the other peer. The peers must acknowledge each packet from the other peer by communicating the sequence number of the received packet.

2.3.6.3 Summary of E-E HIP and UFA HIP mobility management schemes

This section summarizes two HIP-based signaling schemes for UFA, which are responsible for terminal attachment, session establishment and handover procedures. The first scheme, referred to as E-E HIP, applies the original terminal-based approach, where the GWs are not involved in the HIP control functions. The second scheme, referred to as UFA HIP [52], applies the signaling delegation service extensions for reduction of signaling overhead in the terminals and access networks. Table 1 describes the main functions that the HIP control plane provides in E-E and UFA HIP.

Table 1 – Main functions of the HIP control plane in E-E and UFA HIP.

Abbrev.	Description
TA in E-E in UFA	Terminal attachment (TA) occurs when a HIP-enabled host is switched on or is rebooted. The UE executes BEX procedure towards the RVS, as illustrated in Figure 27a. The UE executes a BEX towards the access GW, as presented in Figure 28a.
SE in E-E	Session establishment (SE) covers the HIP signaling procedures related to communication flows between the HIP peers. BEX is triggered before session establishment as long as there is no HA between two peers, as drafted in Figure 27a. The HA is closed (and the SA is deleted) when the SA is unused by upper-layer communication for a period denoted by T_{UAL} or simply by T. T_{UAL} is the minimum of the unused association lifetimes (UALs) configured at the initiator and responder (RFC 5201).

in UFA	In UFA HIP, the same SA pair is used for all communication flows between an UE and its delegate GW, independently of the remote peer. Furthermore, the same SA pair between two GWs provides data protection for all service data flows passing through these GWs, independently from the source and destination peers. During SE, an UPDATE procedure is triggered between the UE and its UFA GW, as long as there is no HA between the UE and the remote peer, as presented in Figure 28b. During that, the GW is notified about the request to establish HA with the remote peer in the name of the UE, and the UE gets feedback on the success of delegated task. In case of lack of SA pair between the GW and the remote peer, a BEX procedure is initiated from the GW to the remote peer in the name of the UE. Otherwise, if the SA pair has earlier been established (by other flows) between the GW and the remote peer, then an UPDATEw/CERT is triggered. If the remote peer turns out to be a delegate GW, then that GW notifies the remote peer about HA creation using an UPDATE procedure.
HO	Handover (HO) covers the HIP procedures for mobility management of a UE. A basic assumption is that GWs publish different IP domains. Handover means that a UE is moving from one IP address domain to another IP address domain, by visiting an access network that is connected to a new GW.
in E-E	If a host gets a new IP address, it sends the address to its peers using an UPDATE procedure (RFC 5206), as illustrated in Figure 27b. This is a reactive mobility management solution.
in UFA	The handover procedure has two phases in UFA HIP as illustrated by Figure 29. The HO procedure in UFA HIP realizes proactive handover. This means that the contexts for data link, network and HIP-layer are established and updated by the control plane in the UE, GWs and the UE's peers before the UE is physically reattached to the next GW. In the first phase of HO (I) the target GW requests the source GW to establish HA with the UE's peers using UPDATEw/CERT procedures. At the end of the phase, the security contexts are transferred from the source GW to the target GW. In the second phase (II) the target GW updates the traffic forwarding policies for the UE at the UE's peers, in the RVS and within the UE itself using UPDATEw/CERT procedures. Therefore the UE's traffic is redirected and passing through the target GW. After that the UE physically reattaches to the new access network.
RV	RVS update (RV) means registration of the fresh locator of a HIP-enabled host at the RVS. The registration lifetime denoted by the symbol T_{RVS} determines the lifetime of an address entry in the database of the RVS.
in E-E	An UE registers its IP address at the RVS right after TA (RFC 5203). Further registrations are triggered due to two factors. First, the registration lifetime T_{RVS} configured at the RVS server determines the minimum frequency of periodic location updates that should be initiated by the UE. Second, during handovers the UE notifies the RVS about its new IP address. The UPDATE procedure is used in both cases.
in UFA	Mandated registrations of the UEs' addresses are triggered during every HO and at every T_{RVS} time by the UFA GWs. The applied procedure is UPDATEw/CERT including the registration request and reply fields.
RK	Rekeying (RK) aims to create fresh keys for a given HA and the related SA pair, using UPDATEw/DH procedure between the peers. T_{KEY} denotes the length of the rekeying period between HIP-enabled hosts.
in E-E	RK may occur between the UEs and between the UE and the RVS.
in UFA	RK may occur between the UEs and their actual serving GW, between GWs and between the RVS and GWs.
DR	Delegation of rights (DR) is present only in UFA HIP. It uses the UPDATEw/CERT procedure involving registration request and reply fields.
in UFA	It occurs in three main cases: first, following the TA, second, when the lifetime of delegation authorization expires, third, during the handovers. In the first two cases the UE registers to the delegation service of its access GW. It generates a temporary public-key certificate for the GW for a certain time called delegation lifetime, denoted by the symbol T_{DEL} in the following. Hence, the GW will be able to sign control messages until the expiration of T_{DEL} in the name of the UE by attaching the certificate of the UE to its signed messages. The third case of DR happens during HO. During HO, either the UE or the previous GW delegates the UE's signaling rights to the next GW. Let denote with the symbol L the maximum certificate-chain length. If the actual length of the certificate-chain is smaller than L before the HO, then the previous GW will propagate the UE's signaling right to the target GW by registering to the delegation service of the target GW, and authorizing it to proceed in the name of the UE. That means that the previous GW appends his certificate to the certificate-chain and conveys that in the CERT field to the target GW. If the length of the certificate-chain is L before HO, then the UE is responsible for the re-delegation of its rights. Hence, the UE will send a new certificate in the CERT field for the target GW with a new lifetime, which will authorize the target GW to proceed in his name.

Figure 27 outlines the terminal attachment, session establishment and handover procedures from the point of view of a UE in E-E HIP. Figure 28 and Figure 29 illustrate the same in UFA HIP. All figures present the triggered HIP signaling procedures and the related control function in parentheses.

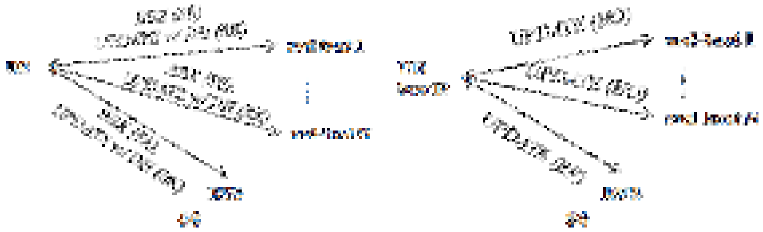


Figure 27 – (a) Session establishment and (b) handover procedures in E-E HIP.

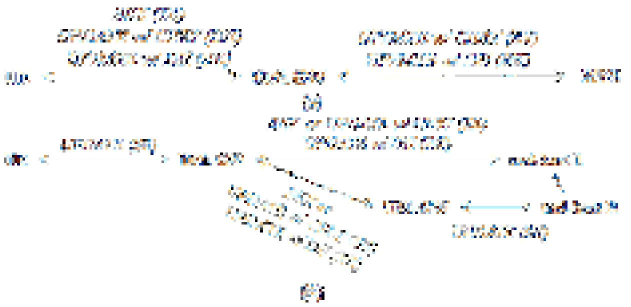
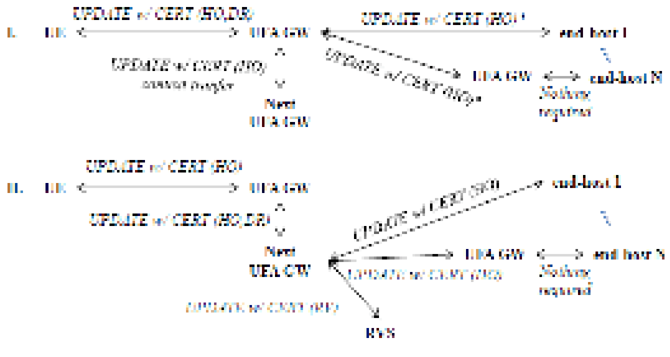


Figure 28 – (a) Terminal attachment and (b) session establishment in UFA HIP based network.



* This procedure is required only if there is no previously established HA between next UFA GW and the end-host (or its delegate UFA GW).

Figure 29 – Handover procedure in UFA HIP based network.

We distinguish three update procedure types for the sake of the analysis of UFA HIP and E-E HIP, because they have different network and node processing requirements.

- UPDATE with DH (UPDATEw/DH) signifies the rekeying procedure, as defined in the standard (RFC 5202). It contains the DH public key values and ESP info from the non-mandatory fields.
- UPDATE with CERT (UPDATEw/CERT) refers to an update containing the CERT field (RFC 6253). It is required in the following two subcategories.

  First, when the delegator, i.e., an UE or a GW, registers to the delegation service of a GW. In this case the CERT field contains the authorization certificate-chain, which authorizes the delegate to act in the name of the delegator in the scope of the authorized roles.

  Second, when a mandated update procedure is initiated by a delegate towards the peer of the delegator. Mandated means that the signaling is performed by a delegate in the name of the delegator. In this case the CERT field contains the authorization certificate-chain, which certifies for a peer that the delegate is temporarily authorized to proceed in the name of the delegator. A mandated update procedure can have any purpose except rekeying. Such purposes are, e.g., registration of the delegator's IP address at the RVS, update of the peers of the delegator with the new IP address of the delegator, or registration of the delegator to the delegation service of a next delegate. A certificate-chain may be too long for one CERT field within on HIP packet, therefore it may be split into multiple CERT fields that are transferred in more than one HIP update messages.
- UPDATE signifies all the other types of update procedures, e.g., registration to RVS (RFC 5203) or location update of the peers (RFC 5206).

3. Related standardization activities

SDN techniques promise to implement simplified management of computer networks by enhancing network automation, increasing innovation through fostered programmability, and reducing CAPEX and OPEX by decreasing costs and consuming less power during operation. The philosophy behind SDN developments is to abstract the underlying communication infrastructure from applications and services by separating control plane functions and roles from data plane and also by centralizing network intelligence and state. SDN researches are very often linked to the OpenFlow protocol, which is a building block of SDN by enabling the creation and maintenance of a global and thorough view on the network itself, and by offering a consistent and pervasive API to dynamically program network devices in a centralized manner.

In this section, we first introduce the industry specification group of Network Function Virtualization (NFV). Then we summarize the trends and challenges of OpenFlow standardization activities in the wireless and mobile domain, describe the main characteristics of SDN-based mobile networks in focus of the ONF efforts, and introduce the most important use cases and key benefits of OpenFlow enabled mobile and wireless communication architectures.

3.1 Network Function Virtualization

Network Function Virtualization (NFV) is a specialized industry specification group (ISG) created by network service providers (AT&T, BT, Deutsche Telekom, Orange, Telecom Italia, Telefonica and Verizon) under the European Telecommunications Standards Institute (ETSI). Activities of NFV involve the implementation of mobile and fixed network functions like firewall/DPI, intrusion detection, different signaling tasks and DNS, all in software. The created virtual, completely software based appliances are therefore aimed to be executed on different, but standardized architectures provided for different network operators by different vendors.

Network Functions Virtualisation is designated to address the problems of shorter HW lifecycles, increasing energy costs, capital investment challenges and other collateral issues of hardware based appliances by leveraging standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises. ETSI NFV ISG believes that Network Functions Virtualisation is applicable to any data plane packet processing and control plane function in fixed and mobile network infrastructures. It is important to note that Network Functions Virtualisation is highly complementary to Software Defined Networking (SDN): these topics are mutually beneficial but are not dependent on each other. Network Functions can be virtualized and deployed without an SDN being required and vice-versa [61].

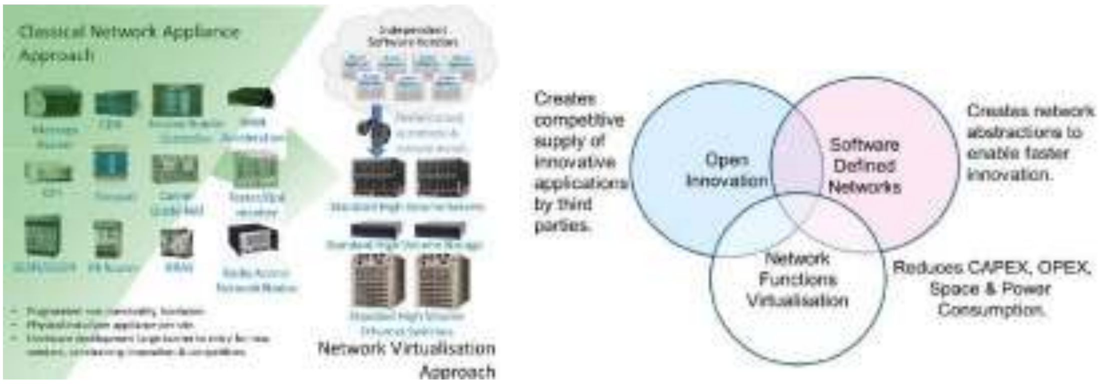

Classical Network Appliance Approach
Independent Software Vendors
Network Virtualisation Approach
Creates competitive supply of innovative applications by third parties.
Open Innovation
Software Defined Networks
Creates network abstractions to enable faster innovation.
Network Functions Virtualisation
Reduces CAPEX, OPEX, Space & Power Consumption.

Figure 30 – Network Functions Virtualisation (NFV) and NFV relationship with SDN [61].

Authors of [62] assume that NFV and in general virtualization techniques will push networking functions currently run on dedicated hardware appliances onto a cloud infrastructure. Expected network functions of EPC to be affected are Mobility Management Entity (MME), Serving Gateway (SGW), PDN Gateway (PGW), etc. With the help of virtualization solutios, EPC could be operated on servers/hyper-visors. In [62] such a mobile architecture is called as a virtualized-EPC or vEPC. A vEPC architecture could potentially offer many benefits including, but not limited to [61]:

- Reduced equipment costs and reduced power consumption through consolidating equipment and exploiting the economies of scale of the IT industry.
- Increased speed of Time to Market by minimizing the typical network operator cycle of innovation. Economies of scale required to cover investments in hardware-based functionalities are no longer applicable for software-based development, making feasible other modes of feature

evolution. Network Functions Virtualisation should enable network operators to significantly reduce the maturation cycle.

- Availability of network appliance multi-version and multi-tenancy, which allows use of a single platform for different applications, users and tenants. This allows network operators to share resources across services and across different customer bases.
- Targeted service introduction based on geography or customer sets is possible. Services can be rapidly scaled up/down as required.
- Enables a wide variety of eco-systems and encourages openness. It opens the virtual appliance market to pure software entrants, small players and academia, encouraging more innovation to bring new services and new revenue streams quickly at much lower risk.

To truly exploit the above potential benefits, there are a number of technical challenges, which need to be tackled [61]:

- Achieving high performance virtualized network appliances, which are portable between different hardware vendors, and with different hypervisors.
- Achieving co-existence with bespoke hardware based network platforms whilst enabling an efficient migration path to fully virtualized network platforms, which re-use network operator OSS/BSS. OSS/BSS development needs to move to a model in-line with Network Functions Virtualisation and this is where SDN can play a role.
- Managing and orchestrating many virtual network appliances (particularly alongside legacy management systems) while ensuring security from attack and misconfiguration.
- Network Functions Virtualisation will only scale if all of the functions can be automated.
- Ensuring the appropriate level of resilience to hardware and software failures.
- Integrating multiple virtual appliances from different vendors. Network operators need to be able to “mix & match” hardware from different vendors, hypervisors from different vendors and virtual appliances from different vendors without incurring significant integration costs and avoiding lock-in.

Though being complementary and sharing two main objectives, namely, openness and innovation, NFV and SDN are two independent paradigms. That is to say, NFV can be implemented without separating the control plane from the data plane as suggested by SDN. However, an NFV infrastructure with SDN support is perfectly conceivable. Even better, it is expected that such an alignment would engender a greater value to NFV, since SDN enhances compatibility, eases maintenance procedures, and provides support for standardization.

3.2 Open Networking Foundation

OpenFlow is a completely open protocol that was originally published by Stanford University researchers in [160] aiming to enable network developers to run experimental protocols in the university campus network. Nowadays, the Open Networking Foundation (ONF)[5], a non-profit industry alliance, is in charge of supporting the researches of software-defined networking and of the standardization activities having OpenFlow in the main focus.

According to the Open Networking Foundation, SDN is an emerging network architecture that decouples the network control and forwarding functions: “Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications” [161]. The Open Networking Foundation is taking the lead in SDN standardization, and has defined an SDN architecture model as depicted in Figure 31.

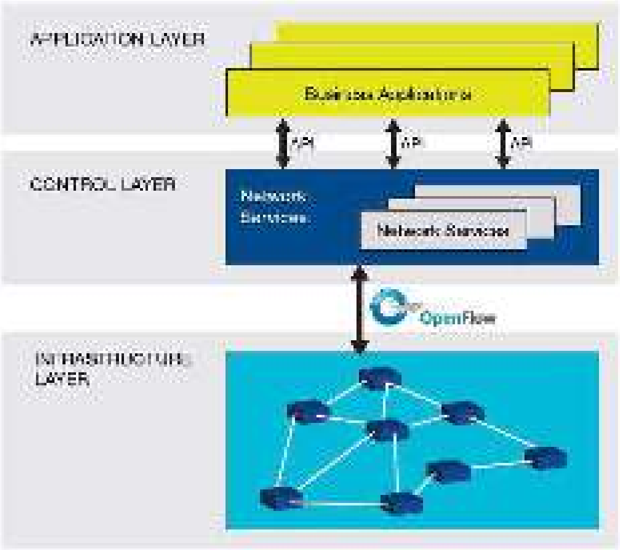


Figure 31 – ONF/SDN architecture [162].

The ONF/SDN architecture introduced in the above Figure consists of three different layers that are accessible through well defined open APIs:

- Application Layer: end-user business applications that consume the SDN services.
- Control Layer: consolidated control functions that supervise the network forwarding behavior using open APIs.
- Infrastructure Layer: system of mainly simple network elements (NE) that provide packet switching and forwarding functionality.

According to this simple model, ONF-based SDN architectures can be characterized by the following three main attributes:

- Logically centralized intelligence: In an ONF-based SDN architecture, network control functions are distributed from forwarding using a standardized southbound interface called OpenFlow. With the help of this, decision-making is orchestrated based on a global view of the overall network or domain, as opposed to existing networks today, which are designed on an autonomous system view paradigm applying nodes that are unaware of the overall state of the architecture.
- Programmability: ONF-based SDN infrastructures are inherently controlled by software functions enabling the management paradigm to be replaced by automation and rapid adoption. Providing open API for this is an important ONF activity to support innovation.
- Abstraction: In ONF-based SDN networks the applications consuming the SDN services are completely abstracted from the underlying network infrastructure and the technologies applied. Moreover, network devices are also abstracted from the control layer in order to grant portability.

3.3 Trends and challenges in the mobile and wireless domain

Infrastructures of mobile and wireless communication exhibit rapid pace of change. The beginning of 21st century witnesses that wireless slowly becomes the primary Internet access method for most people, which

[5] https://www.opennetworking.org/

forces mobile operators to carry higher and higher volumes of traffic and also to deploy more sophisticated services. Over the top video applications can be accounted for the dominant portion of the growing traffic, therefore creating increasing demand for novel network functions like multimedia transcoding, content delivery, and content caching. Moreover, mobile Internet architectures must simultaneously support multiple generations of mobile services (e.g., 3G and 4G) together with a wide set of different user services (VoIP, streaming multimedia, instant messaging, etc.), resulting in varying characteristics of mobile network traffic. Of course these functions and services must be supported in a cost-effective manner.

The expected traffic volume explosion necessitates more cells in the cellular radio access networks (RANs) to provide access of mobile subscriber to Internet resources over the air interface. Operators started to deploy small-cell (pico- and femtocell) technology to increase network capacity through frequency reuse, especially in areas of dense subscriber population. Smaller deployment distances in physical cell spacing are required for higher bandwidths like in 4G LTE, but also one of the most important factors that increase inter-cell interference.

Spreading of simultaneous multi-access environments due to the increasing number of available wireless access technologies is another important trend nowadays. Typical smartphone devices today support 3G and 4G LTE as well as Wi-Fi or Bluetooth connectivity. However, this kind of diversibility in wireless technologies requires mobile network operators to maintain and operate distinct segments of access, backhaul and core networks, increasing both deployment and operational costs. Moreover, carrier networks need flexible deployment options to support migration from older to newer technologies/devices without hampering the user experience.

Providing seamless handovers across such multiple radio technologies is also a challenging task as mobile network operators must apply increasingly complex policies to enforce the the right service through the right access, and also to control handover of sessions between access systems.

Today’s economy provides quicky varying business conditions that require speedy development cicles for new mobile services and also dynamic adoption capability of these services to new technologies. The mobile service and application market is traditionally competitive, but mobile operators struggle with a novel group of competitors nowadays: over-the-top services transmitting ever-growing volume of packet switched data. Besides of these challenges there are also the falling voice revenues forcing mobile operators to replace missing incomeges from new data services like e-commerce, m-commerce, eHealt, mHealth, analytics, advertisements and location based services. Last but not least, network resources must be highly scalable, adaptive and agile despite the fact of increasing capital expenses. All the above demands hardware cost minimalization, enhacments in hardware utilization, and reducing OPEX by applying new technologies and paradigm such as virtualization, cloud computing, softwarization and automation with self optimization.

ONF-based SDN architectures inherit a number of benefits for the above challenges of mobile and wireless environments, including their wireless access, mobile backhaul, and core networking segments. These benefits and potentials are listed below:

- The paradigm of flow-based communication in SDN architectures fits well to provide efficient end-to-end communications in multi-access environments, when different radio technologies, like 3G, 4G, WiMAX, Wi-Fi, etc. are simultaneously available for users. SDN is able to provide fine-grained user flow management aiming to improve traffic isolation, QoS/QoE provision and service chaining.
- Centralized control plane allows for efficient resource coordination of wireless access nodes, which makes possible to implement efficient inter-cell interference management techniques.
- The fine-grained path management in SDN networks provides various optimization possibilities based on the individual service needs and independently from the configuration of the underlying routing infrastructure. In mobile and wireless environments it is really useful as users are frequently changing their network points of access, the used applications and services vary in bandwidth demands depending on the nature of the content to be transmitted, and considering that wireless coverages are providing a naturally chaning environment.
- Virtualization of network functions efficiently abstracts services from the physical infrastructure. Multi-tenancy permits each network slice to possess its own policy, whether that slice is managed by a mobile virtual network operator, over-the-top service provider, virtual private enterprise network, governmental public network, traditional mobile operator or any other business entity.

3.4 ONF standardization use-cases for mobile Internet architectures

Based on the work of Wireless & Mobile Working Group of ONF [162] this section introduces various use-cases defined for wireless and mobile environments that could exploit the benefits of ONF-based SDN infrastructures. The Wireless & Mobile Working Group (WMWG) is chartered to collect such use-cases and determine architectural, protocol and system requirements for extending ONF-based solutions to the wireless and mobile domain. The goals of this standardization working group include optimization and management of different network types including wireless backhaul, 3GPP cellular Evolved Packet Core (EPC), IEEE technologies like OmniRAN or 802.21 MIH, and also unified access and management schemes across wireless and fixed networks. The WG works in a close relation with other technical working groups inside ONF aiming to determine architecture and OpenFlow protocol issues and recommend enhancements to ONF specifications for wireless and mobile use-cases and application scenarios. The WG also intends to initiate and maintain collaboration between ONF and other standardization bodies to further enhance, advertise and ease the use of OpenFlow and ONF-based SDN technologies.

3.4.1 Scalable and flexible EPC

SDN enabled EPC efficiently separates control and forwarding functions, therefore provides flexibility, reliability and user plane scalability. However, control plane centralization should be taken care of.

3.4.2 SDN enable distribution of P/S-GW anchor nodes

Real-life EPC networks are usually deploy centralized and integrated P/S-GW anchor nodes, which serve a big number of eNodeBs, with a serious number of subscribers. Thanks to the user plane anchor behavior, this structure results in a lot back and forth IP traffic in the P/S-GW entities. A distributed or flat P/S-GW deployment with a centralized control nodes (MME, IMS, etc.) could however easily benefit from SDN/OpenFlow by dynamically handling P/S-GW local/mobile IP traffic. This use case describes how SDN and OpenFlow could be applied in distributed/flat EPC architectures, and such helps in reducing back and forth traffic volume and also may decrease EPC OPEX/CAPEX.

3.4.3 Virtualization of S-GW functions

In this use case ONF addresses S-GW virtualization where virtual environment emulates a logically single S-GW with distributed OpenFlow switches. The use-case provides variable efficient resource usage and GW load balancing/overload avoidance. 3 scenarios can be depicted: 1) route optimization between NodeB and P-GW, 2) seamless load balancing, and 3) dynamic GW capacity management for virtualized mobile core.

3.4.4 Unified device management and control

Unified device management proposes to use OpenFlow controller in order to achieve unified device management and control on full outdoor equipment and in door unit, on devices from multiple vendors, on microwave equipments and other types of network devices.

3.4.5 Dynamic resource management in the wireless backhaul

Mobile Internet traffic volume is increasing and with it the requirements against backhaul capacity. As opposed to wired backhaul solutions, wireless backhaul resources are limited and are more vulnerable to the changing environment. In this use-case wireless backhaul resource management is envisioned, that enables the operator to maximize the available wireless resources and minimize the congestion of the traffic also in a heterogeneous, multi-vendor deployment scenario.

3.4.6 Service chaining in the mobile service domain

A service chain consists of a set of network services, like firewalls or application delivery controllers that are interconnected through the network to support a specific service. With SDN, service providers can create service chains aligned to each data type and ensure the level of service each customer purchases. Moreover, moving network functions into software means that deploying a particular service chain (like an e-mail including virus, spam and phishing detection, etc.) no longer requires acquiring new hardware.

3.4.7 Energy efficiency in the backhaul

This use-case aims to optimize power consumption in the mobile backhaul network using the SDN paradigm. Using the OpenFlow controller operator can create a traffic distribution model by real-time traffic monitoring, and based on the measurement results, adaptive and dynamic behavior can be implemented: setting the transmission power level, turning off the radio, etc.

3.4.8 Connection-oriented SDN for wireless small cell backhaul networks

One major application of carrier Ethernet services provided by fixed broadband wireless solutions is the backhaul for small wireless cells. Such wireless backhaul solutions require flexible placement driven by user capacity requirements rather than wired backhaul availability. The IEEE 802.16 Working Group on Broadband Wireless Access deals with the question in Project 802.16r on Small Cell backhauling. An OpenFlow controller may provide the possibiltiy to efficiently select from among multiple 802.16 connections, even supporting a set of various alternative transport techniques.

3.4.9 Optimization of security and backhaul transmisison

This use-case focuses on backhaul optimization based on redundancy elimination. The implementation is based on a chaining concept where specific traffic flows instead of being encrypted, are steered to compressor/decompressor nodes. This use case enables the operator to provide security to crucial flows while optimizing the flows that consumes most of the backhaul resources.

3.4.10 Managing secure IPsec tunnels in LTE

In LTE/EPC networks, existing security procedures apply IPsec tunnels for flow protection. IPsec requires differentiated IP packet processing in network devices based on packet selectors, according to packet header information fields. This is clearly similar to ONF-based SDN operation where the traffic is handled with the help of flow tables. Therefore, flexible handling of IPsec traffic could be implemented by applying the SDN pradigm for enforcing IPsec policies in LTE/EPC architectures.

3.4.11 IEEE OmniRAN

Sharing resources of access and backhaul network segments allows operators to exploit built-in benefits of deployed infrastructures by expanding coverage and decreasing the CAPEX/OPEX. The abstraction of heterogeneous access technologies and creationg of a single access infrastructure from a higher level makes possible the development of novel business cases and provides a customer environment that is totally independent from the network access technologies. ONF and IEEE 802 OmniRAN standardization working groups try to come up with the propoer definition of the open interfaces enabling this scenario by managing and configuring heterogeneous access networks.

3.4.12 802.21 MIH and SDN integration

This use-case relies on OpenFlow to use its efficient flow handling capabilities when managing break-before-make and make-before-break type of flow mobility scenarios by applying the IEEE 802.21 Media-Independent Handover (MIH) protocol. MIH architecture and commands focus on media-independent protocol messages and information elements needed for efficient mobility management, and are under standardization by the IEEE Wireless TG 802.21, particularly including 802.21c for single-radio handover events. As OpenFlow was also specified in a media-independent manner, 802.21 MIH will be very well suited for SDN applications.

3.4.13 SDN-based mobility management for LTE/EPC

IP addresses are semantically overloaded: they used both to identify and locate UEs in the network. A GTP tunnel is spanned over the network to find right location of a UE in case of handover events without the need of changing the actual IP address of a particular UE. This meands that the network is suffering from the overhead of GTP tunnel headers in the user plane, and control plane singling traffic to handle the handovers and tunnel management tasks. However, in an SDN-based infrastructure we could use NodeB's MAC address as locator and UE's IP address as identifier, and set up SDN controllers to maintain the <UE IP, NodeB MAC> table to find a UE based on its IP address. This principle decreases handover singling traffic and eliminates GTP tunnel overhead.

3.4.14 Network-based mobility management

In this use-case the OpenFlow toolset is integrated with well-known network-based mobility management protocols like Proxy Mobile IPv6. These protocols implement mobility management in a way that leaves UEs out from the mobility management tasks as mobile terminals do not require running and executing any mobility/specific functions. This behavior makes UEs able to change their access links while keeping their IP addresses unchanged. It also means that the mobility of UEs generates dynamic IP flows, which can be efficiently handled by centralized SDN control nodes in every mobility domain: the SDN network could easily adapt to the movement of the UEs as the controller will signal the new flow table details to the forwarding elements of the domain, according to the actual mobility situation.

3.4.15 Operator-centric multi-access interface management

Modern UEs are equipped with multiple interfaces, which make users able to choose different radio interfaces for their communication by considering different parameters and factors, like access cost, user experience, user preferences, etc., but without taking network conditions and status into consideration. However, operators would benefit from a network-aware behavior aiming to minimize the transmission cost per byte for UE flows without deteriorating SLA or user QoE by executing a network initiated flow handover to provide Wi-Fi offloading. In this ONF use-case we can define how mobile network operators can use radio interface information and network measurements to drive UE flows to use the multiple radio interfaces to achieve the above goals.

3.4.16 Unified access infrastructure for enterprise and large campus networks

This use case discusses the possibility to implement a unified access network by using the same controller entity to manage both wired forwarding elements and wireless access points using an open interface. ONF lists the requirements of such a framework to run both OpenFlow and CAPWAP (Control and Provisioning of Wireless Access Points) in parallel, by analyzing the gaps of integration with current OpenFlow and CAPWAP solutions.

3.4.17 Inter-cell interference management

LTE and LTE-A are the latest wireless communications standards for cellular mobile networks. They enable high-speed, real mobile broadband data communications. As mobile Internet traffic increases, inter-cell interference leads to more and more significant service degradation in means of user throughput (**Figure 32**). Neighbouring base stations, which result in overlapping cells, required to control and manage their subcarrier allocations in order to avoid interference. The goal is to reduce the signal-to-interference-plus-noise ratio (SINR) using different interference management techniques.

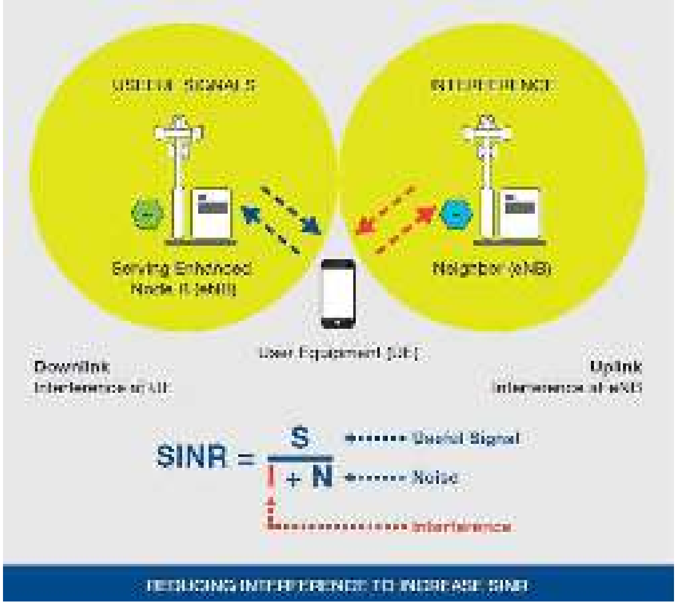


Figure 32 – Inter-cell interference in mobile cellular networks [162]**.**

There are a number of existing techniques applied in LTE and LTE-A networks aiming to cope with the problems of inter-cell interference. Some of these existing solutions are:

- Inter-cell interference coordination (ICIC): selective reduction of power for subchannels in a given frequency domain.
- Enhanced inter-cell interference coordination (eICIC): considers scenarios where macrocells and picocells are overlapping inside a particular coverage area (i.e., to provide hotspots in public places like airports, restaurants, etc.).
- Coordinated multi-point transmission/reception (COMP): decrease interference for edge users of cells by special transmission and reception techniques that utilize multiple transmit and receive antennas from multiple locations, which may or may not belong to the same physical cell. The goal is to enhance the received signal quality and decrease the received spatial interference.

However there are existing solutions, some drawbacks to the current inter-cell interference coordination techniques can be identified. Most importantly, inter-cell interference management in existing LTE/LTE-A networks is achieved using distributed protocols. Solutions, such as the above summarized Coordinated multi-point transmission/reception are quite complex, produce significant processing overhead (thanks to the used distributed graph coloring algorithms that are highly complex and suboptimal) and demand hige power and network resource requirements on the RAN.

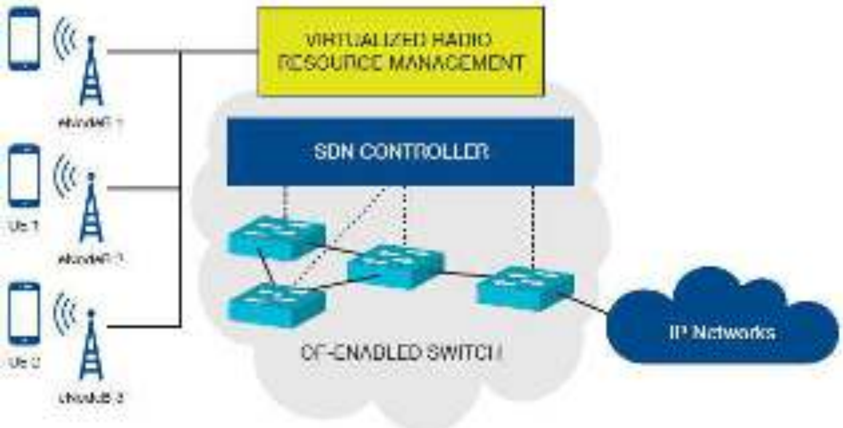


Figure 33 – SDN-enabled eNodeB control for inter-cell interface management [162]**.**

SDN architectures with OpenFlow offer a promising toolset to cope with the abve limitations of inter-cell interference management. Figure 33 depicts a possible SDN-based, logically centralized control layer for radio resource management enabling radio resource allocation decisions to be made with a global view on all the eNodeBs. Such a solutions could be far more optimal than the existing distributed radio resource management (RRM), mobility management, and routing techniques deployed in current mobile Internet architectures. Centralized network intelligence could make RRM decisions based on dynamic power and subcarrier allocation profile of each eNodeB. Moreover, scalability could also be enhanced because as new users are added, the required computing capacity at each base station remains low thanks to the centralized RRM processing inside the SDN controller. Also, a standardized OpenFlow API (i.e., the southbound interface between the SDN controller and the eNodeBs) could ensure efficient hardware abstraction making upgrades to be performed independently from the radio hardware components.

3.4.18 Traffic management and offloading in mobile networks

One of the most straightforward use-case of ONF is traffic steering and path management that have received tremendous attention within the SDN community. Tools of smart traffic steering can be applied for advanced load balancing, load sharing, content filtering, policy control and enforcement, error recovery and redundancy, and in general, any application which involves traffic flow operations and control. Putting all of these potential SDN applications into the context of mobile and wireless networks we gather an other set of potential use-cases like traffic offloading and roaming support, content adaptation (e.g., adaptive streaming solutions), and mobile traffic optimization.

After leaving the voice dominated mobile era, the traffic became a lot more unpredictable: the transition to broadband mobile Internet and the traffic explosion in the audio and video streaming domain resulted in a set of new requirements where the excessive bandwidth demand is the one that barriers profitable network operation. More efficient paradigm is needed to be adopted in mobile Internet architectures helping to scale capacity, ensure optimal use of resources, and to support service differentiation to maximize revenues.

In this SDN use-case, OpenFlow enables mobile Internet traffic to be dynamically and adaptively moved and removed in the mobile network based on a number of possible trigger criteria, such as individual or aggregate flow rate (such as per application or per user user aggregation), aggregate flows number on a particular port or link, flow duration, number of UEs per cell, available bandwidth, IP address, type of application, device utilization rate, etc. All of these criteria can be defined either by the user or by the mobile operator. For example, the operator could measure network conditions and decide to offload mobile traffic in case of need. As a user-centric alternative, subscribers could opt in based on their preferred parameters and pre-defined policies, like: 1) voice calls should never be offloaded, 2) FTP download traffic should always be offloaded to Wi-Fi, etc.

In a more advanced use-case, it could be envisioned that users travel in a multi-access radio environment simultaneously connecting to multiple RANs (perhaps even ones of their choice). Network parameters such as congestion, quality of service (QoS), quality of experience (QoE) are measured, and triggering factors (e.g., a flow rate threshold) are set and changed dynamically by the mobile operator. E.g., “If the flow is an FTP download, and the flow rate exceeds 100 Kbps, hand over the flow from LTE to Wi-Fi.” As the example shows, distinct criteria and thresholds could be applied for different applications and therefore different flow types running on the same UE, or on the terminals of different subscribers. Of course thresholds could be based on the widest range of possible criteria like user/flow profile, location, service plan, etc.

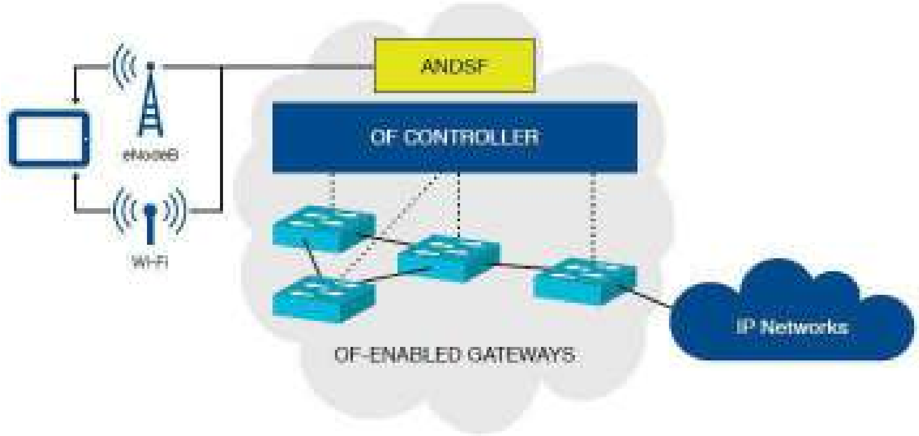


Figure 34 – SDN-based offloading in heterogeneous mobile Internet access environment [162]**.**

Within this scenario, offloading means moving traffic from a 3GPP RAN (e.g., cellular, small cells, femtocell, etc.) to a Wi-Fi access based on operator-centric decision and execution mechanisms. The vertical handover process must be completely seamless (i.e., no data loss or connectivity problem should occur, IP address should be preserved or at least the address change should be seamlessly handled, etc.) to maintain the user QoE. Offloading can also be used in reverse direction, when e.g., congestion on the Wi-Fi network triggers to choose a set of mobile users to be moved to another Wi-Fi acces or to a cellular mobile data connection. If we have a programmable, softwarized environment as depicted in Figure 34, we could enable such intelligent choices and offer a wide range of new services: the SDN controller could interact with network information server entities such as ANDSF (Access Network Discovery and Selection Function) or 802.21 MIH MIIS (Media Independent Information Service) for discovering and select the most appropriate wireless network to the UE/UEs or even individual application flows, and execute the Wi-Fi offload. This use-case requires the mobile network controller (probably residing in the MME), to cooperate with the ANDSF/MISS, and also the framework must provide dynamic information on the actual connectivity details of UEs in all the available RANs.

Mobile traffic management and advanced offloading have become hot topics with the explosion of mobile data traffic because it enables operators to optimize resources, and improve QoS/QoE for high bandwidth mobile multimedia applications and services. However, not only offloading is the only interesting application: wireless link aggregation is also a promising sub scenario, which makes UEs able to bundle available wireless connections and bandwidth to increase aggregated link capacity for UEs. This also requires multi-access mobile devices handling different overlapping RANs at the same time.

4. Challenges and research objectives

This section summarizes the research objectives and main research challenges of resource, traffic and mobility management topics, which we are concerned with in project SIGMONA. The investigated use cases and scenarios are summarized in Section 0.

4.1 Resource management

4.1.1 Combined Virtual Mobile Core Network Function Placement and Topology Optimization

Main targeted benefits

The problem of finding an optimum mapping of virtual nodes and links onto a given physical substrate network is considered as the virtual network embedding (VNE) problem. For VNE, some solutions have been already proposed in the scientific literature as described in Section 2.1.5. These approaches consider the optimum embedding of a virtual network with predefined topology onto a given physical substrate network. Thus, the virtual network topology (graph) itself is fixed and not subject to optimization.

TU Chemnitz focuses on the virtual mobile core network embedding problem and develops a novel approach for combining the optimization of the virtual network topology with the VNE optimization. It relies on the joint embedding of individual core network service chains where a core network service chain denotes the sequence of mobile core VNFs a user or control plane traffic flow has to traverse.

Challenges

- The optimization target is to find a feasible embedding of the core network service chains according to given physical network link/node capacities and capabilities, so as to minimize the total cost for the mobile core network embedding while accommodating the traffic demand. The main challenge here is to construct a suitable linear optimization model for the VNE problem combined with topology optimization, which scales well and is solvable in an acceptable time frame.

4.1.2 Network resource availability awareness in SDMNs

Main targeted benefits

Network resource availability awareness will be the foundation for resource management process, service provisioning and optimization traffic management, as well as security protection and monitoring process.

Challenges

- Heterogeneity of network resources and dynamicity
- Data entities associated to network resources will need a common understanding and common taxonomy
- Network resource management will need a semantic understanding among different software defined solutions
- Adapt current network management platform in order to configure and control the different partner SDN test systems involved, using programmatic resource management and deployment
- Use latest realtime BigData technologies in order to cope with the immediateness and data volumes required

4.1.3 Optimized video delivery

Main targeted benefits

The objective is to enable E2E traffic optimization from client to cloud applications. Network resource demands should be communicated by the applications requiring QoS guarantees to the SDN controller. This research area focuses on the following questions: (1) precisely define the needs of our application towards SDN functionalities to be able to provide such service, (2) study the available SDN REST APIs to check current and future abilities, (3) test current solutions.

Challenges

- To develop application server components to interact with delivery servers and the SDN controller,
- To develop traffic engineering driven via “affinity service” from the SDN controller,
- To ensure development agility to take into account future SDN controller abilities.

4.1.4 In-network caching

Main targeted benefits

In-network caching allows storing the content in a location close to the users, caching permits to reduce the load on the network. The in-networ caching allows to move the cache trought the network. This enables that contents are served from a location close to the users, thus the packets travel less, so the network resources are spared. Caching mainly avoids that requests to the same contents go every time through the whole network to the packet gateways and the interconnections.

Challenges

- Providing in-network caching requires terminating GTP tunnel
- Efficient in-network caching requires proper monitoring and dynami allocation algorithm

4.2 Traffic management

4.2.1 Joint traffic and cloud resource management for service chaining in SDMNs

Main targeted benefits

Creation of high performance service-chaining applications contributes to the fulfillment of traffic demands and higher quality expectations from customers, while reducing capital and operational expenses associated with their networks. To achieve this, traffic should be processed only in the necessary middleboxes and should refrain from processing in unnecessary middleboxes. Detailed identification of each flow, and establishing an appropriate dynamic service-chain for that flow is the main problem. In this project, Ericsson will work on developing an OpenFlow-based SDMN architecture where the SDMN orchestration controller will control not only the flow forwarding hardware, but also the middleboxes that are distributed in geography in the Network-Enabled Cloud by using the traffic and cloud resource management methods.

Challenges

- To develop traffic engineering and service chaining and end-to-end routing application in SDN controller (OpenDaylight)
- Congestion discovery at both routing path and application in cloud.
- Use cloud management system and integrate with controller using API.

4.2.2 Coordinated traffic and resource management and efficient routing in SDMNs

Main targeted benefits

Existing cellular networks suffer from inflexible and expensive equipment, complex control-plane protocols, and vendor-specific configuration interfaces. Compared with wired networks, cellular networks have some unique features and face significant scalability challenges. As networks become more complex and traffic diversity increases, there is the apparent need to manage the traffic carried by the network.

The goal of traffic management is to decide how to route traffic in a network in order to balance several objectives such as maximizing throughput, balancing the link utilization across the network, controlling the bandwidth allocated to competing flows, minimizing latency and ensuring reliable operation when traffic patterns change or parts of the network fail. Different traffic management methods in SDN for wireless networks have been examined in Section 2.2.2. For joint routing/resource management, most common approaches and techniques are heuristics. Mixed Integer Linear Programming (MILP) is also often used since the problem’s nature is NP-hard. Approaches using graph theory and multi-commodity flow is examined as well but may not take into account all of the requirements of the problem. Other approaches are based on game theory, multi-agent systems, self-organization and policies.

Challenges

- The goal is to provide resource allocation techniques for mobile networks exploiting virtualization in regard of content-aware, operator centric, optimal treatment of user traffic with appropriate QoS/QoE and possibly with appropriate energy consumption.
- After allocation of resources by intelligent heuristics, the principles of control theory and/or game theory can be applied to further manage bandwidth and routing resources for varying traffic conditions.
- The analysis of the optimization possibilities for the existing traffic and resource management solutions/algorithms and examination of their suitability for heterogeneous mobile network architecture will be performed for the designed semi-distributed algorithms.

4.2.3 Application-level traffic optimization in SDMNs

Main targeted benefits

By the integration of ALTO network information service into SDNs ALTO becomes transparent for the UE or the service claimant entity (no deployment cost in the UE). Due to ALTO information, the ALTO client in the SDN controller can overwrite the initial peer selection decision of the service claimant entity (e.g. UE). Any flow can be dynamically selected for getting ALTO guidance and SDN provides built-in redirection mechanisms.

Challenges

- Development of ALTO client in SDN controller, realization of ALTO Client-to-Server interface defined in the ALTO protocol specification and ALTO server
- Implementation of flow redirection to selected peers with Redirect server
- Implementation of routing in and beyond SDN-based network areas
- Implementation of ALTO Server-to-Network APIs, automatic network map provision, cost map provision, and merging of map information
- Selection of ranking aggregation technique for ALTO guidance based on multiple cost types: it is an interesting research question, which kind of ranking method should be used for ranking candidate endpoints for a given service class. There exist many multi-attrbiute decision making methods in the literature, such as weighted sum, weighted product, analytic hierarchy process, multiplicative analytic hierarchy process, distance of ideal alternatives etc and our objective is to provide guidance in the selection of ranking aggregation technique when multiple cost types and criteria must be considered resulting in different rankings of the alternatives.

4.2.4 SDN-controlled IP wireless mesh network

Main targeted benefits

This research topic addresses the opportunity of offloading the Radio Access Network by the use of IP Wireless Mesh Network (e.g. WiFi Ad Hoc). Here we consider SDN control of IP communications in the edge networks, meaning that smartphones and fixed gateways are SDN capable. It is commonly assumed that such a target would be handled by end-terminals themselves as a completely distributed system without mobile network supervision. This research topic investigates wether the mobile network operator can keep control of these communications to redirect traffic to a different access network (e.g., fixed).

Challenges

- Specify solutions to allow coordinated and efficient IP Wireless Mesh communications between end-terminals (such as smartphones) by a supervisor.
- Define a software architecture to provide support of SDN on smartphones and lightweight mobile devices.
- Specify and implement topology control algorithm for such kind of network
- Specify the adequate parameters (such as proximity with a fixed gateway) allowing controller to take decisions about the most effective topology for the network.

4.2.5 Secure mobile data offloading in SDMNs

Main targeted benefits

The benefits of a secure mobile data offloading research are mainly related to the significant improvement of the networks capacity. Offloading part of the traffic from the SDMN network will result in an important increase of the available resources efficiency when the system is coverage limited, capacity limited, or both.

Challenges

- Analyze the data handling to manage the secure mobile data offloading over SDMN.
- To characterize the additional capacity, which can be obtained by network operators when including opportunistic offloading techniques.
- Analysis of the data handling, in order to manage the secure mobile data offloading over SDMN.
- Understand how traffic requested by the users should be managed in presence of hybrid infrastructures (WiFi-LTE-SDMN).
- Maximize the gain for the operator in terms of saved bandwidth and network capacity through the design of efficient offloading protocols.
- Find a distributed trust and security model that allows the network topology to change remaining it secure and trustful.

4.2.6 DiffServ QoS in SDN-based transport

Main targeted benefits

DiffServ QoS architecture can provide soft QoS guarantees on top of different Layer-2 technologies in a scalable manner. However, in current SDN standards (e.g., OpenFlow, OpenFlow Configuration) QoS management is still in early stage. Our research will focus on the discovery of QoS capabilities of SDN-transport (traffic classification, shaping, policing, dropping), in order to provide QoS guarantees in (partially) virtual network forwarding paths of MNOs and VMNOs.

Challenges

- DiffServ QoS may provide a scalable QoS enforcement service providing soft QoS guarantees. It may enable both flow separation and sharing of supplementary link capacities. Provision of DiffServ QoS services is possible with multi-level priority queues.
- Current ONF specifications (OpenFlow, OF-config) do not support multi-level priority queues, only, one-level, flat priority queues using a simplified version of hierarchical token bucket filter and hierarchical fair-service queues.
- QoS should be guaranteed on virtual mobile network level, with enough granularity. Traffic aggregates mapped to different QoS classes may represent e.g., different service classes for the MNO, entire traffic of a mobile network slice, or service classes per mobile network slices. We will investigate with measurements the traffic management capabilities provided by different multi-level priority queues. It is challenging to define the appropriate level of granularity.
- Interaction with PCRF, and the mapping of 3GPP QCIs to the Diffserv QoS classes which can guaratee dynamic policy control for traffic separation is also an important challenge.

4.2.7 Quality of Service enforcement in SDMNs

Main targeted benefits

The QoE Managaement framework ISAAR can benefit from adding SDN functionalities. The quality monitoring of Internet services starts with identification of the respected flows within the traffic mix. Normally a lot of processing is needed for this detection, due to the Deep Package Inspection (DPI) required. To simplify that mechanism the OpenFlow (OF) matching rules can be used. Therefore, the OF controller has to be configured in a way which allows identifying measurable traffic by using the matching rules and teeing it out to one of the measuring points of ISAAR in real-time. This flow selective copy port mechanism allows for traffic steering of the relevant packets towards centralized measurement probes. On the other hand OF functionalities can be used for changing the per hop behaviour (PHB) for each traffic flow.

Challenges

- To realize a comprehensive traffic monitoring and enforcement with only few measurement points the traffic has to be crossed out and transported to that measurement points
- Current SDN implementations like Open flow are lacking of priorization functions for specific traffic flows
- The signaling between the points of presence within the network and the measurement points has to be defined and the additional network load has to be analysed
- Interaction with PCRF, and the mapping of 3GPP QCIs to the Diffserv classes and other markings, which can be used for traffic enforcement on flow level is also an important challenge.

4.3 Mobility management

4.3.1 Extension of HIP-based DMM solutions for scalable and secure mobility management in SDMNs

Main targeted benefits

By the integration of centralized and/or distributed anchors (of post-DMM solutions) with the SDN forwarding functions QoS/QoE driven mobility management and support of complex mobility scenarios will be supported.

Challenges

- What are the performance gains of delegation-based HIP signaling scheme over the E-E HIP signaling scheme in distributed mobile network environment. Several engineering questions must be answered regarding the optimal settings of HIP lifetime parameters and number of GWs in E-E HIP and UFA HIP. During the adjustment of those parameters, the main objective is to keep low the signaling overhead.

  - An interesting question is, e.g., the influence of the setting of a HIP parameter, called unused association lifetime (UAL), on the overhead. UAL gives the length of idle communication period between two HIP end-nodes after which the protocol deletes the HIP HA and IPsec SA pair. Higher UAL results in longer SA periods, hence lower SA establishment (HIP Base Exchange, BEX) rate, but increased number of IPsec SA and HIP HA entries that must be stored in the memory of HIP nodes. Moreover, it increases the overall rekeying rate in the system. Rekeyings are triggered at constant periods during the lifetime of SAs. Both BEX and rekeying contain the computationally demanding ephemeral Diffie-Hellman (DH) key exchange procedure, therefore reduction of their rate is essential.
  - Another interesting question is related to the delegation of signaling rights. How many levels of delegations, i.e., propagation of signaling rights from delegate to delegate, should be enabled, and how should the original delegator set the expiration time of such an authorization certificate (i.e., the delegation lifetime T_{DEL}). These parameters influence the average length of delegation certificate-chains conveyed together with public-key signatures in mandated update procedures, hence influence the load of the network elements and transport network.
- How SDMN addressing conventions and options can support deployment of UFA HIP GW entities in a loosely coupled SDMN – UFA HIP integration scenario.
  - Loosely coupled integration of SDN technologies and the UFA HIP scheme considers scenarios where OF switches are not HIP-aware, they only provide a transparent transport service for HIP signaling and user plane messages. However, it is an open question how SDMN addressing techniques, conventions and options will emerge, and whether these SDMN addressing schemes will support deployment of UFA HIP (and any post DMM solution), or modifications are required for such integration.
- What are the performance characteristics of HIP-capable OF switch based UFA HIP operation in a tightly coupled SDMN – UFA HIP integration scenario.
  - Tightly coupled integration of SDN and UFA HIP considers HIP-aware OF switches where Host Identity Protocol (and its UFA HIP extensions) are operating as a novel and flexible secure control and user plane with advanced DMM solution for SDMNs. The most important question in this scheme is the applicability: what are the performance limitations of such a novel, HIP-based SDN mobility architecture.

4.3.2 Proxy MIPv6 in SDMNs

Main targeted benefits

This topic investigates the concrete evolution of the standardized Proxy Mobile IPv6 (PMIPv6) mobility management protocol for SDN-NFV architectures.

Challenges

- Addressing of the specification details for efficient integration of PMIPv6 into an SDMN infrastructure (e.g.: integration with service chaining, coordination with the orchestrator, etc.),
- handling of the SDN control plane,
- emulation of network functions (Mobile Access Gateway – MAG, Local Mobility Anchor - LMA),
- relocation of the LMA function on a per user basis.

4.3.3 OpenFlow-based mobility management for heterogeneous SDMNs

Main targeted benefits

Purely SDN-based mobility management solutions provide mobility transparency to higher layers even without applying additional tunneling. Advanced mobility scenarios and fine-grained mobility management is to be supported within heterogeneous (3GPP/non-3GPP) access environments using a clean, OF-only mobility management solution.

Challenges

- SDMN integrated ANDSF – OpenFlow solution for 3GPP-compliant handover optimization in heterogeneous SDMN access environments.
  - ANDSF is specified in the 3GPP standards to provide information to assist non-3GPP access network selection and to facilitate efficient inter-technology handovers in 3GPP/non-3GPP context. However ANDSF is also a promising tool for SDMNs, very little previous work is available on the topic of ANDSF and OpenFlow integration. Support of flexible and adaptive network controlled, OF-driven IP flow mobility, location-based optimization of access nework discovery and smart access selection for UEs in SDMN environments are the main challenges to be solved within this topic.

- SDMN integrated IEEE 802.21 MIH – OpenFlow solution for obtaining link information and controlling link behavior, in an access-independent manner for 3GPP/non-3GPP heterogeneous SDMN access environments.
    - 802.21 MIH provides an extended set of features for handover optimization compared to ANDSF. There are published works that rely on the extreme flexibility of SDN mechanisms in order to desing and develop OpenFlow extensions for control and manage wireless links through Media Independent Handover mechanisms. However, none of the published efforts managed to map the proposed OF based MIH-aware mobility management schemes into the LTE/EPC protocols. Mapping IEEE 802.21 primitives together with the integrated OpenFlow-based mobility management extensions to LTE/EPC will offer new perspectives to network designers for enhancing future softwarized mobile networks (SDMNs).

4.3.4 Enabling secure network mobility with OpenFlow

Main targeted benefits

Mobility offers many dazzling opportunities that also bring with them some profound challenges related to security and privacy. We argue that mobile IP has limitations against DoS, passive eavesdropping, insider attack, replay ttack, tunnel spoofing and location privacy [3]. Security in IP based networks is widely tackled with a common set of protocols composed of secure file transfer protocol (SFTP), secure socket layer (SSL), and transport layer security (TLS). OpenFlow enables an acceptable level of security with SSL or TLS though; it does not support mobility [4]. These limitations insist modifications to the current OpenFlow architecture. More specifically, below we describe the major problems of present OpenFlow version.

- Flow processing: Change of address would disrupt flow processing from network switches. Thus, require regular updates to flow tables.
- Secure session management: Changing an IP address may also tear down active SSL/TCP sessions.
- Secure handover: Problem of mutual authentication and reauthentication. SSL way cannot support mobility alone and certificate exchange would not be preferable for fast moving OpenFlow clients.
- Flow rule management: Change of IP address to solve latter issue causes additional overhead, since flow rules must be updated frequently.

The test bed attempt the address the previous problem by enabling identity locator separation in the SDN control plane.

Challenges

As far as the sessions are built on top of the IPs which are dynamic and highly reluctant to change with mobilit. Furthermore, use of another identity such as media access control (MAC) address is excessively vulnerable, since it can be easily replicated in a virtual machine. The latest implementation of OpenFlow version 1.0.0 uses TLS version 1.0 on top of TCP which is too fragile due to mobility. Thus, the challenge now it to come up with a different solution but without a performance drop or secure vulnerability due to mobility.

- Redirection: This aspect is generally addressed by providing some sort of re-direction mechanism to enhance the traffic steering already provided by basic routing. Redirection can be achieved by replacing the destination address with a surrogate address that is representative of the new location of the end-point. Different techniques will allow the redirection of traffic either by replacing the destination's address altogether or by leveraging a level of indirection in the addressing such as that achieved with tunnels and encapsulations.

- Scalability: Most techniques create a significant amount of granular state to re-direct traffic effectively. The state is necessary to correlate destination IP addresses to specific locations, either by means of mapping or translation. This additional state must be handled in a very efficient manner to attain a solution that can support a deployable scale at a reasonable cost in terms of memory and processing.

- Optimized Routing: As end-points move around, it is key that traffic is routed to these end-points following the best possible path. Since mobility is based largely on re-direction of traffic, the ability to provide an optimal path is largely a function of the location of the re-directing element. Depending on the architecture, the solution may generate sub-optimal traffic patterns often referred to as traffic triangulation or hairpinning in an attempt to describe the unnecessary detour traffic needs to take when the destination is mobile. A good mobility solution is one that can provide optimized paths regardless of the location of the end-point.

- Client Independent Solution: It is important that the mobility solution does not depend on agents installed on the mobile end-points or on the clients communicating with these end-points. A network based solution is highly desirable and is key to the effective deployment of a mobility solution given the precedent of the large installed base of end-points that cannot be changed or managed at will to install client software.

- Address Family Agnostic Solution: Since mobility relies on the manipulation of the mapping of identity to location, address families with lengthier addresses tend to provide alternatives not available with smaller address spaces. These address dependent solutions have limited application as they usually call for an end to end deployment.

4.4 Basic assumptions for resource, traffic and mobility management

This section collects basic assumptions, which provide guidance to the research work in the resource, traffic and mobility management related research directions and objectives.

Table 2 assigns the research topics of SIGMONA WP3 with the basic assumptions of the project. The table also contains some short reasoning in the Notes column.

Table 2 – Mapping of basic assumptions to use cases

Basic assumptions	**Use cases**	**Notes**
Assumption on Migration: Compatibility with the legacy systems vs. Clean-slate deployment	DiffServ QoS in SDN-based transport Post-DMM, PMIPv6-SDN SDN-based mobility management Coordinated traffic and resource management and efficient routing in SDMNs: Clean Slate	Compatibility with legacy systems: keep PCRF, provide compatiblity with MIP/PMIP-based legacy solutions; SDN support of GTP tunneling Clean-state: purely SDN-based mobility
Assumption on network functionality: Virtualization and running functions in cloud	ALTO-SDN DiffServ QoS in SDN-based transport Post-DMM, PMIPv6-SDN SDN-based mobility management Coordinated traffic and resource management and efficient routing in SDMNs	Network Functionality: Network Functions in the Cloud; Keep delay budgets (e.g., service interruption times due to HO)
Assumption on Quality of Service: QoS provision in virtualized mobile core networks in SDN-based network forwarding paths	ALTO-SDN DiffServ QoS in SDN-based transport Post-DMM, PMIPv6-SDN SDN-based mobility management Coordinated traffic and resource management and efficient routing in SDMNs Optimized video delivery for BVS in SDN	QoS enforcement is needed in SDN transport, reduce impact of mobility on QoS, dynamic QoS-aware routing in SDN . In non-SDN domains we should keep 3GPP QoS enforecement
Assumption on mobility management: SDN-based mobility management versus 3GPP and MIP mobility	Extesnion of legacy solutions: Post-DMM, PMIPv6-SDN SDN-based: SDMN integrated ANDSF/802.21 MIH (SDN-based, but using legacy components, e.g. ANDSF); Secure network mobility	SDN-based mobility management: SDN support for GTP tunneling / exchange of GTP tunnels with SDN paths. Legacy mobility management and tunneling Post-DMM use-case aims to provide compatiblity with legacy tunneling solutions, e.g., MIP/PMIP-based legacy solutions, utilize ANDSF etc
Assumption on locator and identity assignment to UEs in SDMNs: the current practice will not change even if P-GW-C is virtualized vs. new identity/locator assignment solutions are needed	ALTO-SDN Post-DMM, PMIPv6-SDN SDN-based mobility management Coordinated traffic and resource management and efficient routing in SDMNs	Current practice will not change in terms of IP address distribution mechanisms for end-hosts: IP distribution is assumed to not change in short or mid-term; Influence of Identity /locator separation as a part of mobility management in IP networks ;
Assumption on Delay-Security Constraints: Optimize security setup to reduce delays	DiffServ QoS in SDN-based transport Post-DMM SDN-based mobility management Secure network mobility	Optimized security setup to reduce delays: security synchronization with global identities; authentication /reauthentication and context transfer during mobility; Security mechanisms might influence OF signaling procedures (flow mapping to queues, traffic policing)
Assumption on network monitoring: NM should be aware of network virtualization vs. NM should not be adapted to network virtualization	ALTO-SDN DiffServ QoS in SDN-based transport Post-DMM SDN-based mobility management Coordinated traffic and resource management and efficient routing in SDMNs	Network Monitoring: Aware of Network Virtualization. Or use cases may require information from network monitoring

Assumption on availability of resources: Resource availability awareness is the foundation for resource management process, service provisioning and optimization, traffic management as well as security protection and monitoring process.	Resource availability awareness based on SDMN In-network caching	Network resources availability: Physical and virtualized resources (managed by MNO and MNVO) will require to have updated information on available inventory and topology.

5. Use cases and scenarios

This section defines the use cases and scenarios of dynamic resource, traffic and mobility management functions in SDMNs.

5.1 Resource management

5.1.1 Combined Virtual Mobile Core Network Function Placement and Topology Optimization

This topic focuses on the joint embedding of individual core network service chains where a core network service chain denotes the sequence of mobile core VNFs a user or control plane traffic flow has to traverse. This relaxation is feasible as the mobile-to-mobile traffic share has only a minor impact on the virtual mobile core network topology and on the placement of the VNFs due to the fact that most of the traffic in mobile networks is caused by Internet applications. All embedded service chains together then comprise the virtual mobile core network.

In our optimization model, a service chain is further decomposed into a user plane service subchain (TAP - SGW - PGW - IXP) and several control plane service subchains (TAP - SGW), (MME - HSS), (MME - SGW).

The traffic demand is specified as follows: for each core network service chain the (user and control plane related) bandwidth requirements on the virtual links between the VNFs as well as the processing, storage and switching (throughput) resources the VNFs pose on physical nodes are given.

The optimization target is to find a feasible embedding of the core network service chains according to given physical network link/node capacities and capabilities, so as to minimize the total cost for the mobile core network embedding while accommodating the traffic demand. We formulate the objective function as a linear combination (with weight factors) of three cost terms:

- Basic cost that occurs if any VNF is placed on a physical substrate node,
- cost per occupied storage, processing and switching unit on a physical substrate node and
- cost per occupied capacity unit on a physical link.

5.1.2 Resource availability awareness in SDMNs

Network resource availability awareness is in the focus of this use case. The use case, illustrated in Figure 35, will identify both physical and virtualized network resources, populating an inventory showing topology and availability of resources deployed, also including the traffic and resources needed for the deployment of the secure data offloading.

The use case proposes a network resources monitoring platform in order to get visibility of the different partners' SDMN systems.

The management platform is fully horizontally scalable, both, in the device management and event storage.

Use case will employ latest real time BigData technologies in order to cope with the immediateness and data volumes required. Being based on a high availability and scale out configuration, it will be able to cope with the most demanding programmatic configuration tasks, covering the most demanding usage scenarios.

- Information regarding virtual and physical networks will be collected for status monitoring and to be presented in a GUI
- Requires appropriate functions in SDN controller and SDN switches

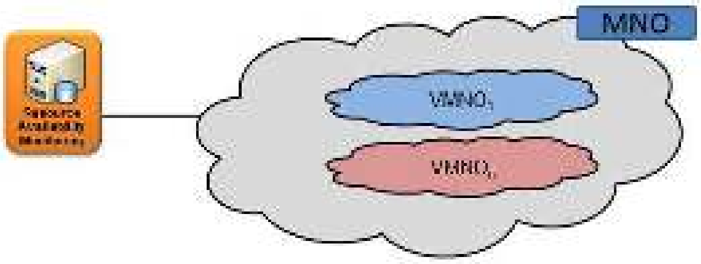


Figure 35 - Resource availability monitoring

5.1.3 Optimized video delivery

The main principle of the use case is depicted in Figure 36.

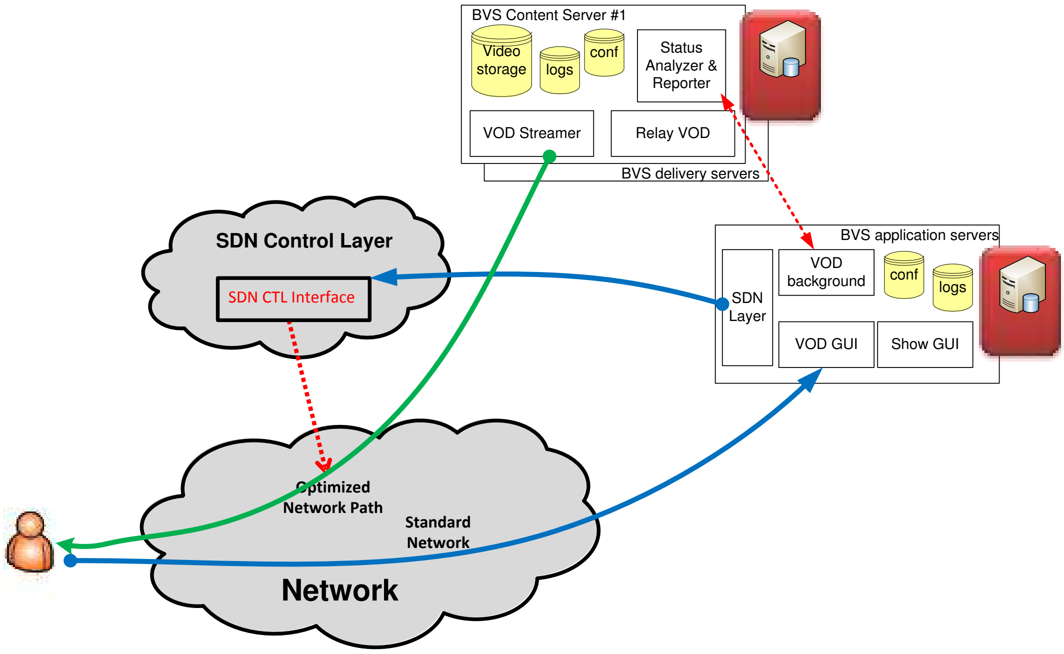


Figure 36 –SDN use case, HTTP video streaming scenario.

The scenario is divided into three main steps:

Step 1: The End-User is connecting to a BVS application servers to select a video to play on his terminal,

Step 2: The application asks the SDN interface to setup an optimized network path from one of the video content servers and the End-User's terminal

Step 3:Video is played on the End-User's terminal, streamed by the selected delivery server

The detailed sequence diagram of the scenario is depicted in Figure 37.

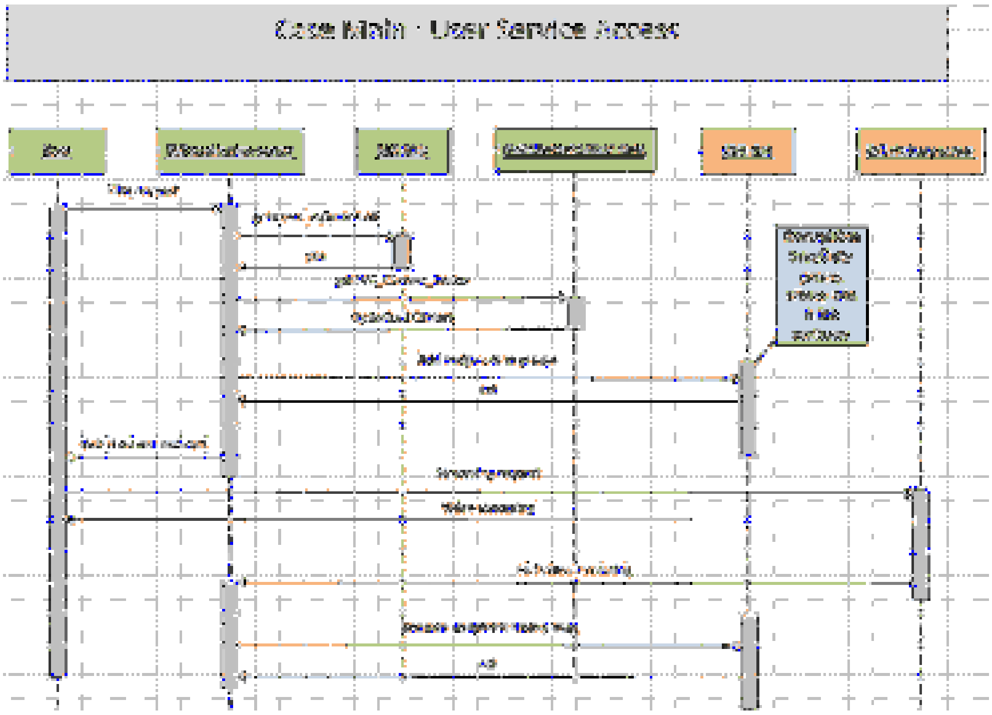


Figure 37 – Deatiled sequence diagram of HTTP video streaming scenario in SDN environment.

Required functions from the SDN layer:

- to set up affinity service according BVS application server requirements (groups, link and attributes). Inputs:
    - Affinity groups: a list of endpoints, which identifies application interfaces or users. All endpoints within a given affinity configuration are assumed to be within a single layer 2

domain at the current stage of the implementation,
    - Affinity links: connection between two groups with a given policy,
    - Affinity link attributes: define how flows should be handled. Attributes are aligned with a given SLA.

- to open a network path with min/max bandwidth from a delivery server to an end-user. Inputs:
    - the end-user terms (IP),
    - the delivery server terms (IP),
    - the min/max bandwidth (Mbps)

- to free an existing network path (ie. Remove endpoints from groups). Inputs:
    - the end-user terms (IP),
    - the content server location (IP)

5.1.4 In-network caching

The first and most relevant advantage is that caching reduces the network traffic and the bandwidth consumption. The requests are served from a local copy, thus they do not go across the whole network to fetch the content from Internet. Thus, caching reduces the network load and the peering costs since less volume is going in and out of the network. Another advantage is that serving the content from local copies improves the users' experience by reducing the latency. The cache allows retrieving the content from a close location so the round-trip time (RTT) is lower for the local cache than for the original web server.The caching also increases reliability since the connection does not go across multiple links through the uncertain Internet. Another positive point is that caching reduces the load on the servers by load-balancing the requests on the different caches. Thus caching can also enhance the robustness of the service since in case the web server goes down, the contents can still be served with the local copy stored in the cache. However, caching can have drawbacks too, since it increases the latency in case of a cache-miss (content not stored yet) or in case of non-cacheable content. Caches can also be a bottleneck or a single point of failure if the design is not done carefully.

We present use case on how SDN is used in the context of the SDMN after removing the GTP tunnels and enable caching in any location of the backhaul networks.

The architecture used for the test case has been inspired by the ContentFlow solution. It is composed of several elements, including caches, proxies, a SDN controller and a cache controller. The proxies include a request analyzer, to get the URL requested, and is thus referred to either as a proxy or an analyzer. In this testbed, the topology is defined and does not change so some related static rules are set on the switches.

Figure 38 presents the first testbed, composed of a single client (for a base station), a proxy, a SDN controller, a cache controller and two caches. The tests were performed with three configurations:

- Without any caching, directly fetching the content from internet.
- With caching in a first cache.
- With caching in a cache closer to the client.

The tests have been performed by adding latency and reducing bandwidth on the link between the two parts of the network.

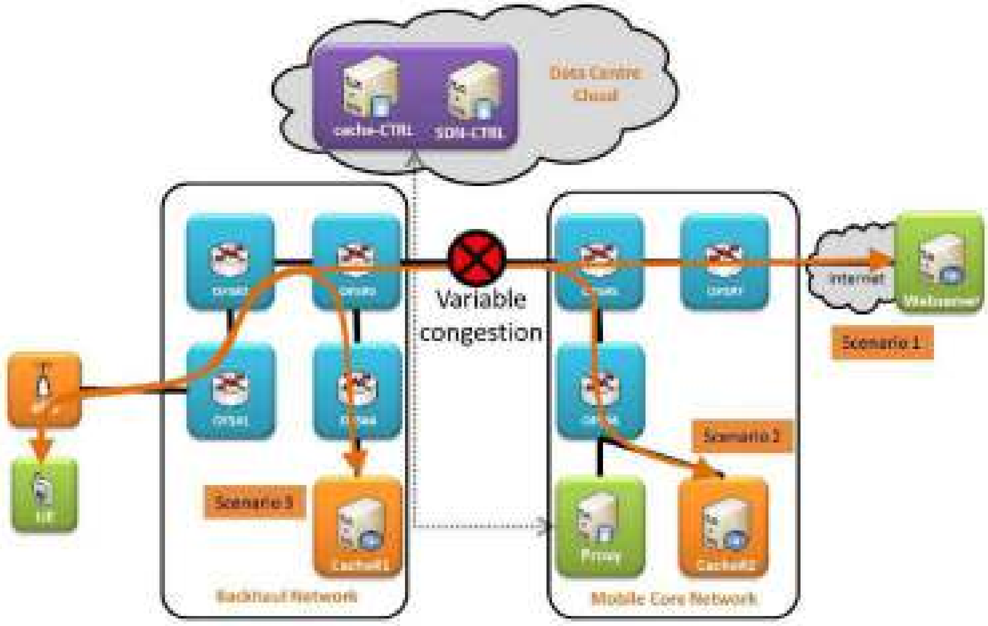


Figure 38 - Demonstration scenarios of the SDN caching implementation.

5.2 Macroscopic traffic management

5.2.1 Joint traffic and cloud resource management for service chaining in SDMNs

An explosive growth in the data traffic necessitates higher capacities in the mobile network infrastructure. Thus, networks are becoming more difficult to manage. In this situation, operators try to meet users' and enterprise expectations with higher performance, ubiquitous connectivity, lower operational cost. Services which are provided by operators have to become more efficient to handle competitive market and fast rollouts are required.

In addition to provide those services there are many network applications such as firewalls, content filters, intrusion detection systems (IDS), deep packet inspection (DPI), network address translation (NAT), content caches, load balancers, wide-area network (WAN) accelerators, multimedia transcoders, logging/metering/charging/advanced charging applications, etc. already existing in today's networks. Such applications are generally referred to as middleboxes, because they are commonly executed along the traffic path, with their existence usually unknown by the end users. In fact, almost all traffic in mobile networks visit a pre-defined sequence of middleboxes en route to its destination today. Such a sequence is commonly referred to as a "service chain". Then, a service chain consists of a set of network services that are interconnected through the network to support an application such as VoIP, streaming video, e-mail, web browsing, etc. In other words, service chaining "orchestrates" the network flow for every offered application.

Creation of high performance service chaining applications is essential to meet traffic demand, higher quality expectations from customers while reducing capital and operational expenses associated with their networks. To achieve this, only necessary middleboxes should be processed. Detailed identification of each flow, and establishing an appropriate dynamic service-chain for that flow is the main problem.

In this project, Ericsson will work on developing an OpenFlow-based SDMN architecture where the SDMN orchestration controller will control not only the flow forwarding hardware, but also the middleboxes that are distributed in geography in the Network-Enabled Cloud as illustrated in an example in Figure 39. A service chain application running on this controller will be developed that will jointly optimize:

- participating middlebox selection
- dynamic chain adaptation based on results from executed middleboxes
- corresponding end-to-end routing

for different user, subscription, application, geography, and context data so that user perceived quality is maximized, network congestion and middlebox overload probabilities are minimized.

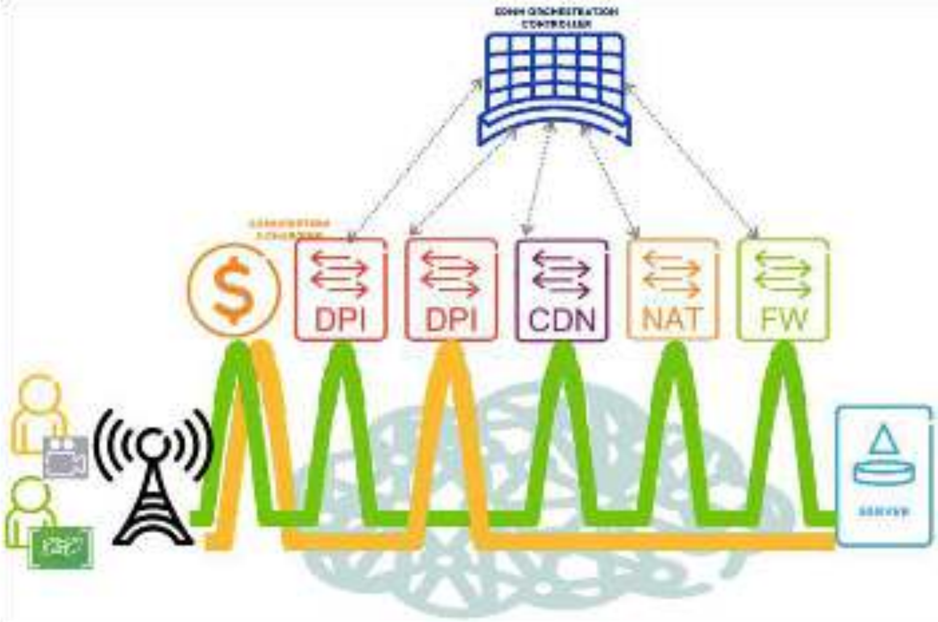


Figure 39 - Example of Middlebox Selection.

Ericsson's modifications of existing standard mechanisms have been depicted in Figure 40.

Developing an SDMN service chaining orchestration to cover all possible scenarios is not realistic, therefore Ericsson will focus on the below described use cases within SIGMONA.

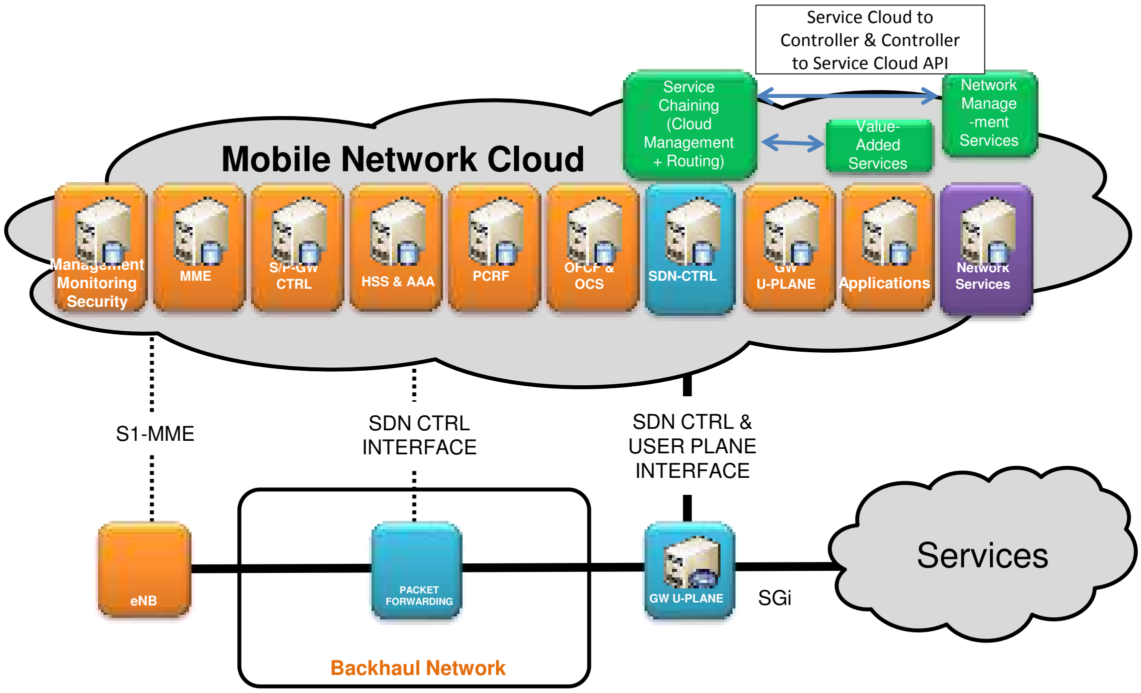


Figure 40 - Ericsson's modifications of existing standard mechanisms.

5.2.1.1 Service chaining use case 1: Selecting video transcoder according to QoS requirement and routing efficiency.

Network providers may sell high quality video subscriptions to customers or may want to differentiate quality based on specific applications (youtube, facebook etc.). Video transcoder in the service chain can be selected accordingly via the SDN controller.

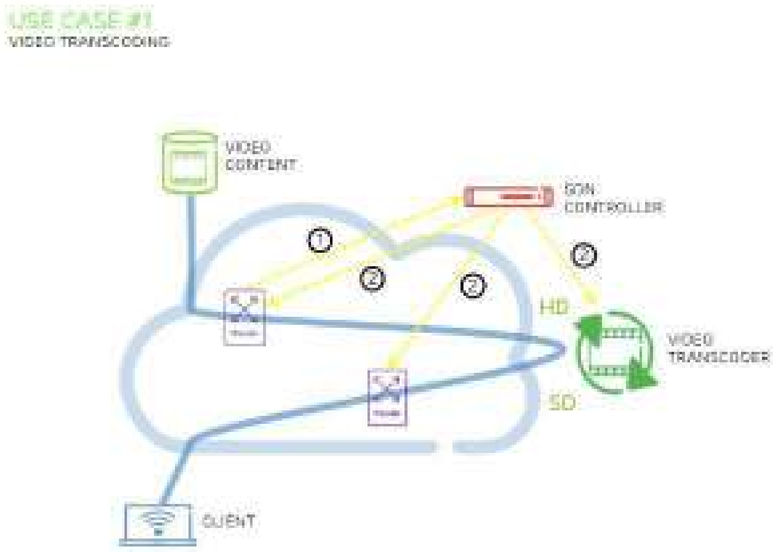


Figure 41 - Service chaining use case 1: Selecting video transcoder.

1) The router queries the SDN controller on how to proceed with a new "video streaming" flow.
2) SDN decides based on (i) user profile (subscription details, device capability) and/or (ii) network congestion map, decides on a "service chain" for this flow.

It pushes the necessary <Match,Action> rules to the routers to facilitate the Service Chain.

It manages the Video Transcoder service by determining its instance and specifying it with the necessary information (flow details, conversion details, etc) using the new "Controller to Service Cloud API."

5.2.1.2 Service chaining use case 2: Ad insertion over video.

Network providers may want to insert ad over video according to user profile.

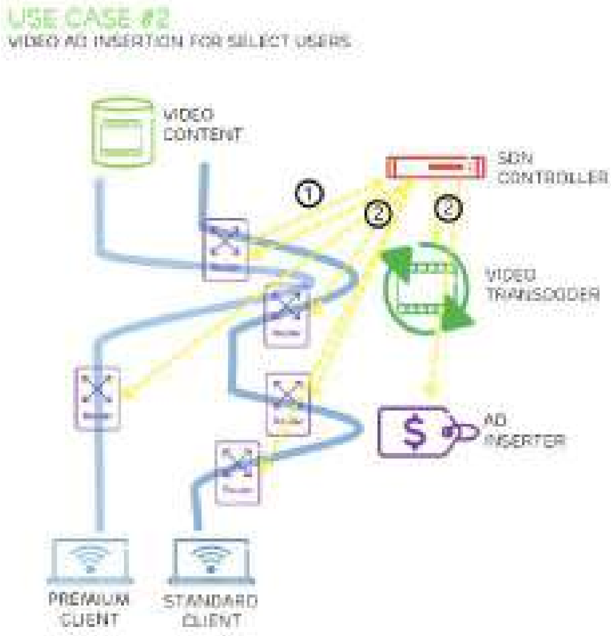


Figure 42 - Service chaining use case 2: Ad insertion over video.

1) The router queries the SDN controller on how to proceed with two new “video streaming” flows, one for a standard user and another for a premium user.

2) SDN decides based on (i) user profile (subscription details, device capability) and/or (ii) network congestion map decides on a “service chain” for this flow.

It pushes the necessary <Match,Action> rules to the routers to facilitate the Service Chain.

It manages the Video Transcoder service by determining its instance and specifying it with the necessary information (flow details, conversion details, etc) using the new “Controller to Service Cloud API.”

It manages the Video Ad Insertion service by determining its instance and specifying it with the necessary information (flow details, ad details, etc) using the new “Controller to Service Cloud API.”

5.2.1.3 Service chaining use case 3: Ad insertion over web content flow.

Network providers may want to insert ad over web content flow according to user interst as illustrated in Figure 43.

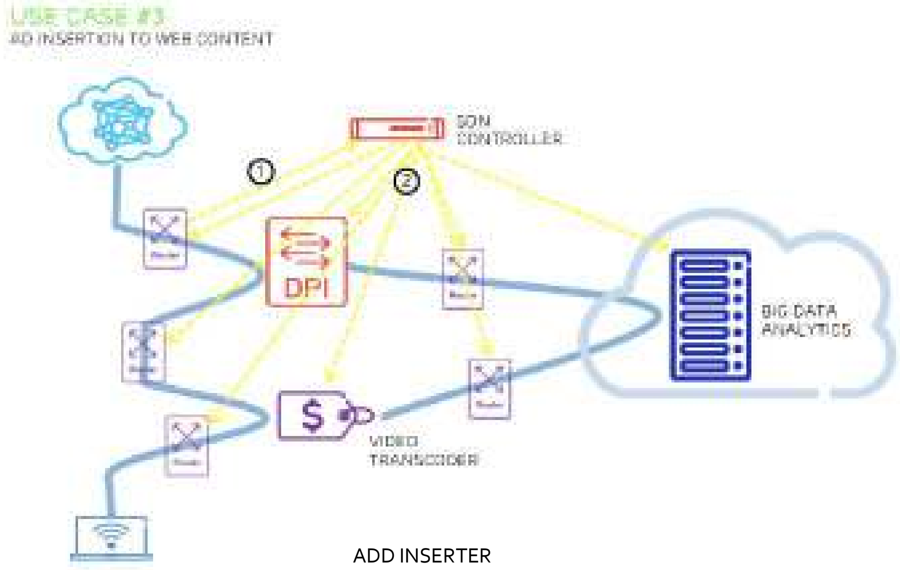


Figure 43 - Service chaining use case 3: Ad insertion over web content flow.

1) The router queries the SDN controller on how to proceed with a new “web content” flow.

2) SDN decides on a “service chain” for this flow that contains DPI followed by Big Data Analytics that instigates Ad Insertion into the content.

It pushes the necessary <Match,Action> rules to the routers to facilitate the Service Chain.

It manages Big Data Analytics service by determining its instance in the Cloud and specifying it with the necessary information from DPI (flow details, where to place the ad, etc) using the new “Controller to Service Cloud API.”

It manages the Ad Insertion service by determining its instance and specifying it with the necessary information (flow details, user specific history, ad details, etc) using the new “Controller to Service Cloud API.”

Architectural requirements of Ericsson use cases:

- SDN controller
- SDN Switches
- Applications
- Network Services
- Management,Monitoring, Security

5.2.2 Coordinated traffic and resource management and efficient routing in SDMNs

The optimization problem of the coordinated routing algorithm will be defined considering the traffic load in software defined mobile networks.

- When the traffic load is high: the main objective is to satisfy users’ QoS requirements for a given power constraint.
- When the traffic load is low: the main objective is to reduce operational costs (such as the power) for given users’ QoS constraint.

For SDMN’s, we will implement the following scenarios depicted in Figure 44 and Figure 45 by using Matlab and/or NS2/NS3.

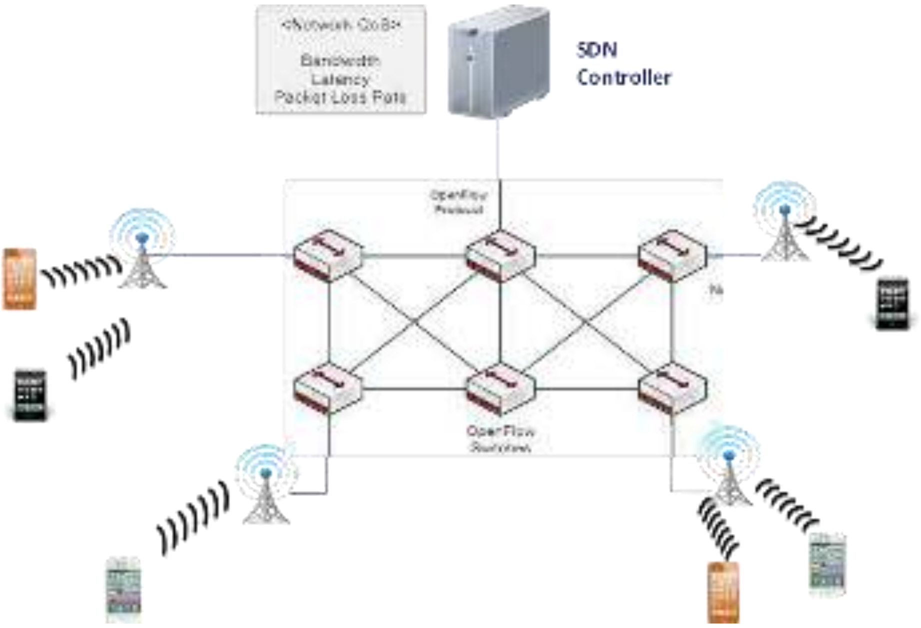


Figure 44 - The first scenario for SDMN.

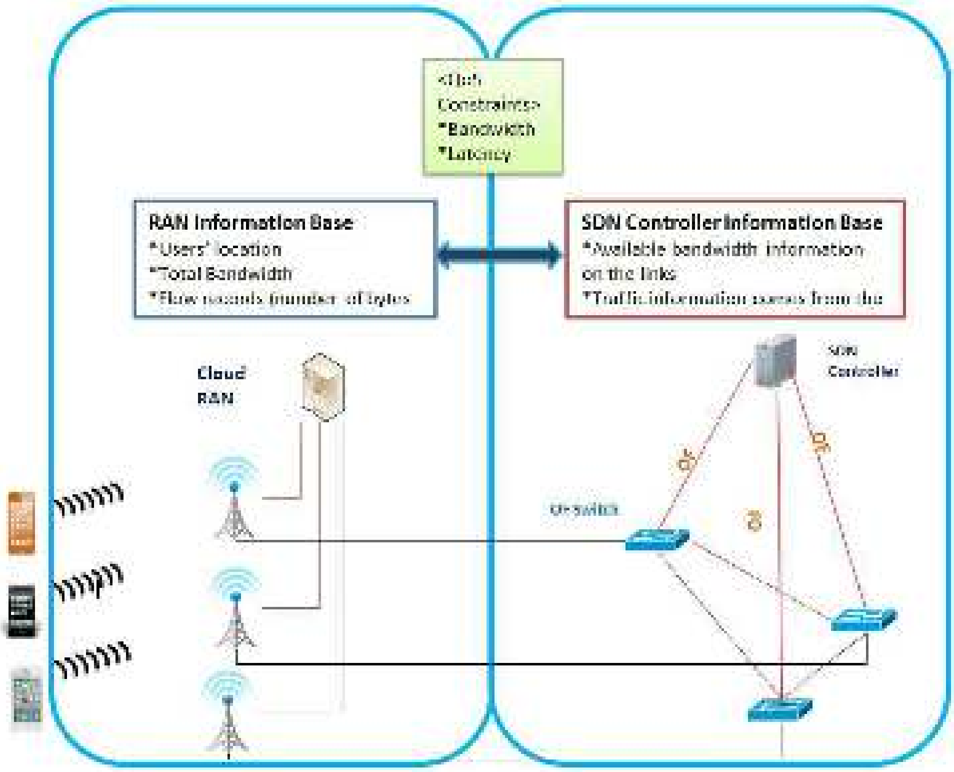


Figure 45 - The second scenario for SDMN.

5.2.3 Application-level traffic optimization in SDMNs

Figure 46 illustrates the use case where ALTO guidance is used for better-than-random endpoint selection for HTTP-based video streaming service.

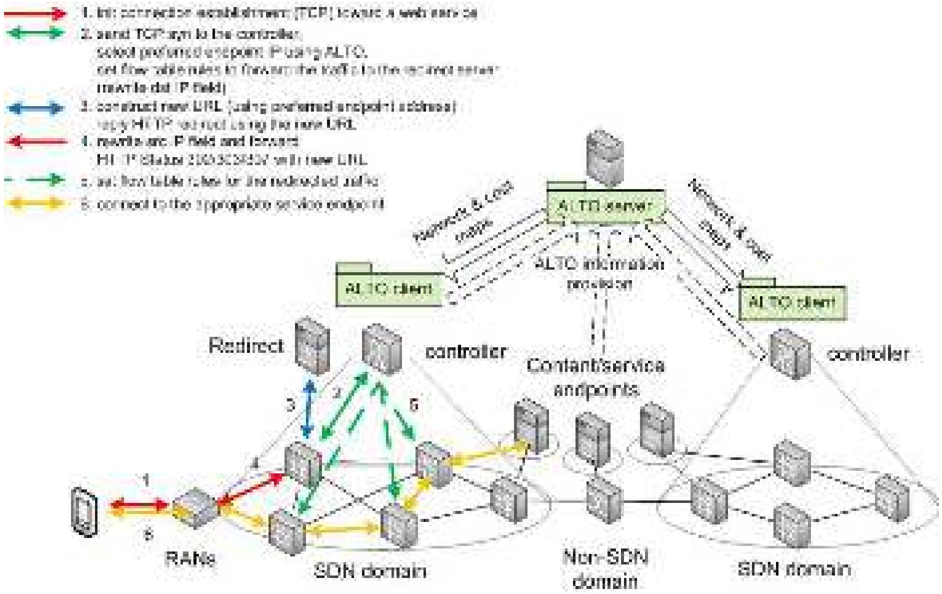

1. Init connection establishment (TCP) toward a web service
2. send TCP syn to the controller,
select preferred endpoint IP using ALTO,
set flow table rules to forward the traffic to the redirect server
(rewrite dst IP field)
3. construct new URL (using preferred endpoint address)
reply HTTP redirect using the new URL
4. rewrite src IP field and forward
HTTP Status 301/302/303/307 with new URL
5. set flow table rules for the redirected traffic
6. connect to the appropriate service endpoint
ALTO server
Network & cost maps
Network & cost maps
ALTO information provision
ALTO client
ALTO client
Redirect
controller
controller
Content/service endpoints
1
2
3
4
5
6
RANs
SDN domain
Non-SDN domain
SDN domain

Figure 46 – ALTO-SDN use case, HTTP video streaming scenario.

The SDN controller shall be notified about a new TCP connection establishment request by the edge SDN-switch of the SDN domain. Since ALTO network and cost maps basically apply IP addresses, and not, HTTP URIs, the IP and TCP header of TCP SYN message shall be used to decide, whether this connection should get ALTO guidance or not. If yes, then the ALTO client shall find the appropriate network and cost maps for the service, and shall determine the candidate IP addresses/PIDs for the service. If not already cached, it may request the appropriate maps from the server with target-independent query. Next, the ALTO client may, calculate k-shortest paths for each cost-type. That is followed by a multi-attribute ranking procedure to calculate the aggregated ranking of the endpoints.

We point out that there exist multiple ways to perform rank aggregation; hence it is an interesting question, which aggregation method should be used. Ranking typically requires normalization or scoring under each cost type. The normalized scores can then be aggregated with a ranking aggregation technique based on weights of cost-types and the achieved scores under cost-types. Common methods for normalization are sum-based, maximum/minimum-based, vector-based normalizations, and common methods for score aggregation are eWeighted Sum, Weighted Product, Logarithm of Weighted Product, Analytic Hierarchy Process, Multiplicative Analytic Hierarchy Process, Grey Relational Analysis, Distance to the Ideal Alternative, and Technique for Order Preference by Similarity to Ideal Solution. A subtopic related to this scenario is to evaluate multiple ranking methods.

After that, the ALTO client and SDN controller shall check resource availability for candidate paths to the best endpoint. If the E-E path crosses multiple SDN domains, this would require communication over the west-east interfaces interconnecting SDN controllers.

Then, the SDN controller shall install the necessary flow entries in its SDN domain, and notify other SDN controllers on the path to do the same for this flow.

If the procedure does not find any path toward one of the endpoints, the TCP SYN should be dropped. If the service can support IP address rewriting, the controller should instead rewrite the destination IP address downstream and the source IP address upstream.

Another option is that the TCP connection (and the HTTP communication on top of that) is redirected to a local HTTP redirect server. The related flow entries must only be kept until the HTTP redirect server redirects the source to the appropriate endpoint; hence these are very short-lived flow entries.

The HTTP redirect server must be notified about the selected IP address, and may resolve the DNS name to generate the new HTTP URI for the client. Then it can send the HTTP redirect message back to the client.

5.2.4 SDN-controlled IP wireless mesh

Adressing the objectives described in Section 4.2.4, this use case investigates opportunities to offload 3GPP Radio Access Network by the use of IP Wireless Mesh Network using SDN capable smartphones. CEA LIST is developing a new SDN southbound protocol for fine-grained wireless performance monitoring.

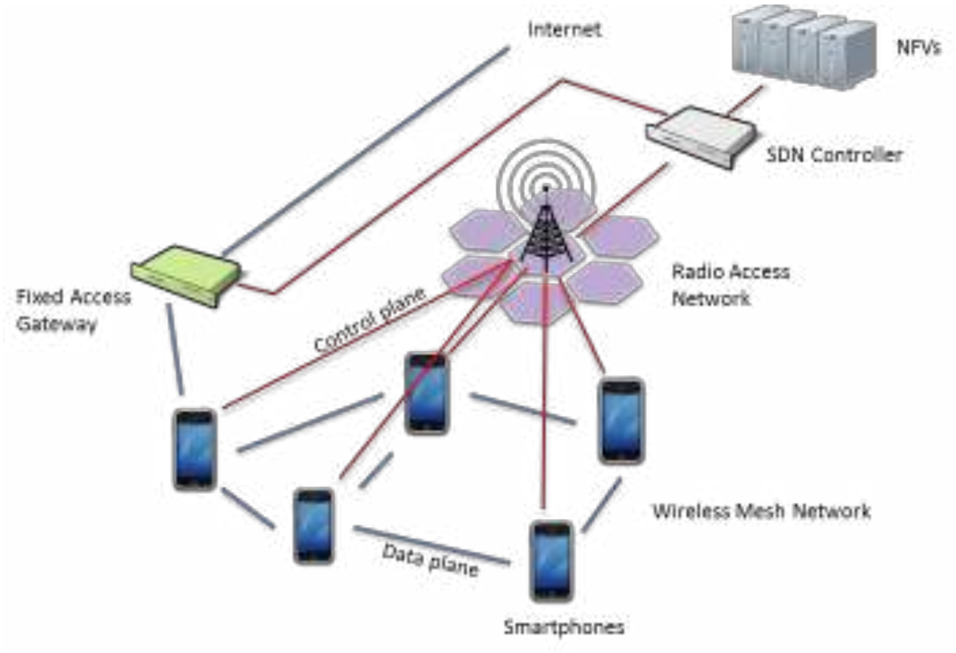


Figure 47 - Communication architecture for the SDN-controlled Wireless Mesh Network

As presented in Figure 47, the use case targets to demonstrate establishment and control of an IP wireless mesh network by the use of NFV supervisor (through SDN control plane). The selection of an alternative access network gateway (for instance a fixed access point – a home premise box) could be the root point for the creation of an IP wireless mesh network with neighbouring end-terminals.

5.3 Microscopic traffic management

5.3.1 DiffServ QoS in SDN-based transport

In this use case we plan to implement an interface between legacy PCRF and SDN controller for QoS enforcement using the DiffServ approach. This requires the modification of standard QoS policy enforcement, described in Appendix B.4.2.2.

A network-intiated QoS control procedure has the following steps in current 3GPP architecture:

1. Application level signaling between the UE and the AF (e.g., SIP, SDP).
2. Session information provision from the AF to the PCRF (over the Rx reference point). In case of IMS services, the SDP information is mapped to QoS information, such as bitrate, service type.
3. The PCRF may request subscriber-related information from the SPR.
4. PCRF makes policy decision based on session information, operator-defined service policies, subscription information and generates PCC / QoS rules.
5. PCC rules are pushed by the PCRF to the PCEF and PCEF enforces the policy and charging rules, and, conditionally, if BBERF is required, then QoS rules are pushed to the BBREF and installed.

In SDMN environment, two operation modes can be implemented for policy control, transparent and non-transparent. In case of transparent approach the user does not have to communicate with the AF. It is the controller, which signals information on arriving sessions to the PCRF through the Rx interface. In case of non-transparent mode, the first two steps remain the same as they are now, i.e., the user signals to the AF its requirements.

In both modes the last step (step 5) is different from the legacy control procedure. The control messages on the Gx interface are translated to flow entry pusher REST API messages at the northbound interface of the controller. PRFF can dynamically create and delete flow entries for traffic aggregates. The following figures illustrate the two operational modes. Both require the translation of Gx messages, therefore our first aim is to implement the translation of Gx messages to flow entry pusher messages.

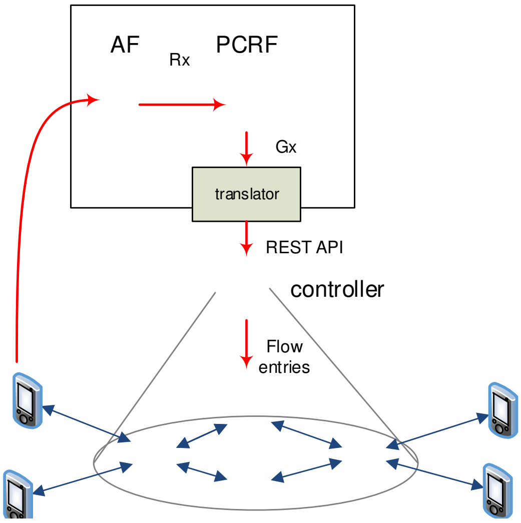


Figure 48 – Policy control (non-transparent mode)

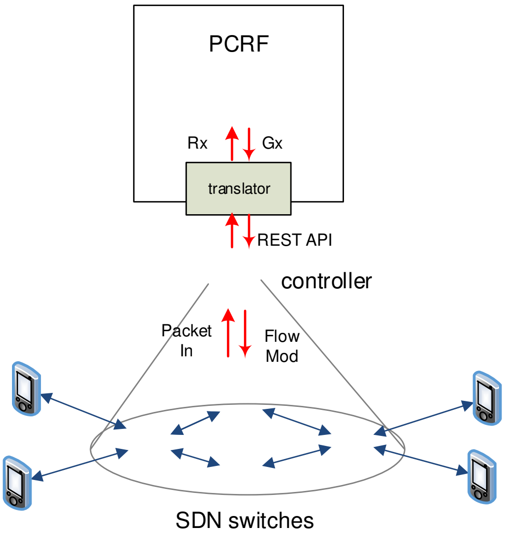


Figure 49 – Policy control (transparent mode)

5.3.2 Quality of Service enforcement in SDMNs

5.3.2.1 QoE Enforcement (QEN)

The enforcement of the PFB is done in the third functional block of ISAAR, "QEN". For data streams with a certain QRULE determines the PFBs and QEN reacts accordingly by applying suitable mechanisms to influence the transmission of the involved data frames or packets. There are several ways to enforce the required behaviour. The first one is to use the PCRF/PCEF in mobile networks and trigger the setup of dedicated bearers via the Rx interface. A second option is to deploy layer 2 and layer 3 frame/packet markings. Based on these markings a differentiated frame/packet handling (scheduling, dropping) is enforced in the network elements which are traversed by the frames/packets (per hop behaviour). In case a consistent marking scheme across all layers and technologies is ensured by the QRULE entity, the QEN does not need to change the existing configuration of the network elements. With GTP tunnels in place, the priority marking has to be applied within the GTP tunnel as well as outside. The outside marking enables routers to apply differentiated packet handling also on GTP encapsulated flows without requiring a new configuration. For IPsec encrypted GTP the marking also has to be included into the IPsec header. The inner and outer IP markings are set in downstream and in upstream direction based on the flow information (five tuple) and the PFB obtained from QMON. As a third option - in case that the predefined packet handling configuration of the routers should not be used - the ISAAR framework is also able to perform a fully automated router configuration. With that, the QEN may explicitly change the router packet handling behaviour (e.g. packet scheduling and dropping rules) to influence the flows. With the SDN approach a fourth possibility to influence data flows is realised by using OpenFlow features. For example, the priority of a flow can be changed in the forwarding configuration directly in an OpenFlow switch action list configuration. Furthermore, flow-specific traffic engineering could be realized. In order to use the OpenFlow features for flow enforcement ISAAR is connected to the control interfaces of the SDN switches.

5.3.2.2 Demonstrator

To illustrate the QoE measurement a demonstrator was used to process an example HD YouTube video for MOS calculation. The demo setup consisting of 3 Laptops which are forming the SDN Switch and SDN Controller another laptop where the QoE monitor was running and 2 PC which are generating background traffic is shown in Figure 50. The video is streamed from the Video Server to the Video client trough the SDN setup. The video traffic is copied out to the QMON device, which is evaluating the QoE of the video flow. The video detection is done by matching rules within the SDN switch. The switch is also used to change the priority of the video flow in case of high traffic loads. Therefore, two queues have been created inside the switches: one for the video stream and one for other traffic. The SDN switch sorts the data packets into the right queue due to matching and action rules, which are configured by the controller.

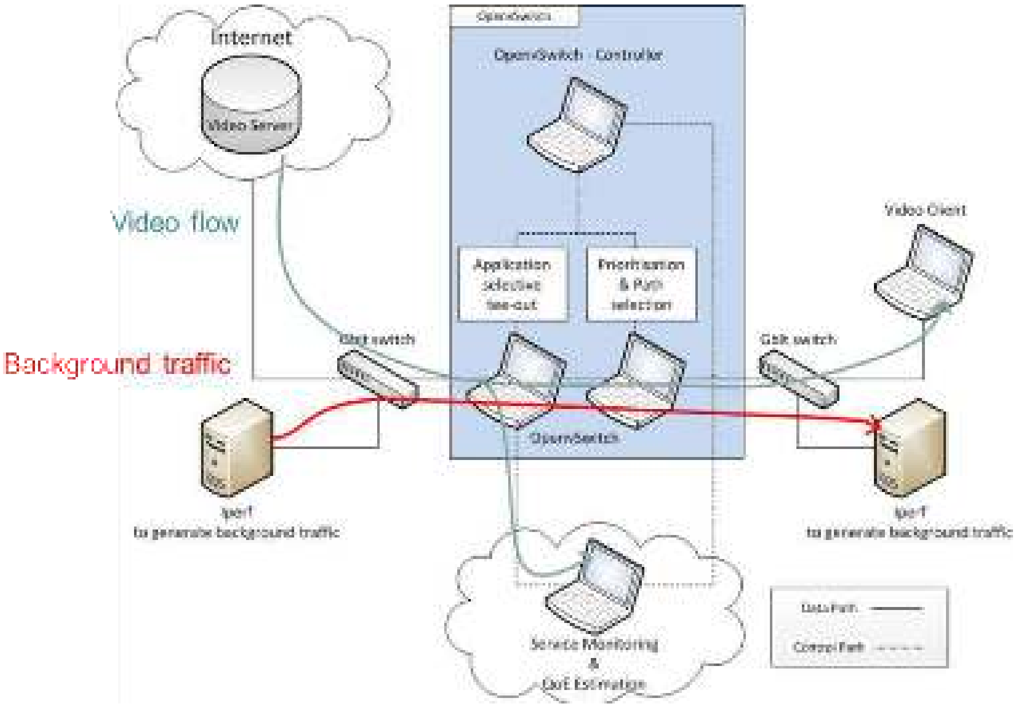


Figure 50 - SDN demonstrator setup.

Within the test the Video Buffer was set to 10 seconds. The outgoing line to the video client has a data rate of 2Mbps, the used Video has an average bitrate of 800kbps and the background traffic is set 1.4Mbps. Therefore, without any traffic engineering the line has to get congested due to an overuse of 200Kbps. In this experiment, no background traffic is applied to the network, only the video was transmitted. The SDN matching as well as the SDN enforcement had been switched of in that test. In Figure 51 it can be seen that the video buffer is filled with a plenty amount of data during the whole video playback, due to the 2Mbps line which is only used by 800Kbps. Hence, there have no stalling events occurred and the QoE was not decreased.

The second test is driven out without the SDN functionality but with applied background traffic. The results are shown in Figure 52. It can be seen that after the initial buffer event the video playout is consuming the buffered data until the buffer level hits the zero line. In this moment the video gets stuck and the MOS value and with it the QoE is decreasing. The stalling event itself reduced the QoE and the negative impact gets even higher each second the video is not playing. Therefore, the MOS value is falling until the video playback is restarted. After the playback is resumed the memory effect kicks in and the MOS value is increasing as long as the video is playing. In the figure three major and a shorter stall of the video can be seen, each new stall effects the QoE more than the previous one. For a high video quality such stalls have to be prevented.

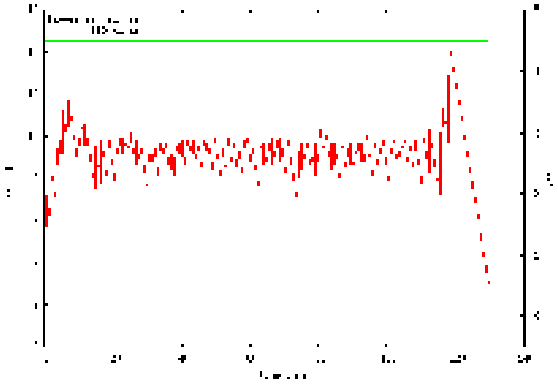


Figure 51 - Buffer fill level without background traffic without SDN

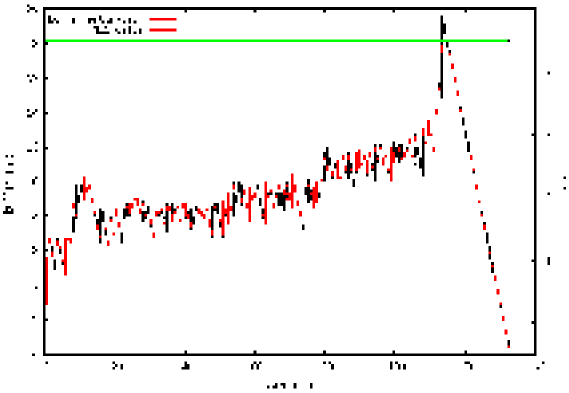


Figure 52 - Buffer fill level with background traffic without SDN

Figure 53 - Buffer fill level with background traffic with SDN

However, now we applied the SDN QoE enforcement, the results can be found in Figure 53. The line is still limited to 2Mbps and the background traffic is set to 1.4Mbps the video bit rate is not changed, too. But the video traffic can be put to another "high quality" queue by the SDN controller. Therefore, the video buffer is filled with sufficient data over the whole video playback and no stalling events occurred. The demonstrator shows that it is possible to use SDN functions to detect specific traffic, copy it out and enforce the needed QoE to it.

5.4 Mobility management

The first two use cases integrate existing distributed mobility management solutions, i.e., UFA HIP from literature and standard PMIPv6 into the SDMN architecture. The third solution combines proactive, media independent handover protocols with purely SDN-based mobility management. The fourth use case is targeting secure network mobility using SDN-capable switches.

5.4.1 Extension of HIP-based DMM solutions for scalable and secure mobility management in SDMNs

5.4.1.1 Modeling the signaling overhead in Host-Identity Protocol-based secure mobile architectures

We have introduced an analytical model for the analysis of overheads of HIP-based procedures in distributed mobile network architectures with the objective of determining the performance gains of delegation-based scheme, UFA HIP, compared to the E-E HIP scheme.

The details of the modeling have been described in [147]. Based on our model, we performed a detailed performance analysis of E-E and UFA HIP mobility schemes, those results are detailed in [148].

5.4.1.2 Coupling UFA HIP and OF-based SDMN technologies

In this use-case (Figure 59) UFA HIP managed HIP/IPsec tunneling is applied to replace standardized tunneling options between GWs and between UEs and GWs. However, for 3GPP and trusted non-3GPP access, OpenFlow-based path management would be required between the PoA and the first UFA GW. The solution supports seamless inter- and intra-GW handovers due to proactive OpenFlow and HIP mobility, multihoming and UFA-HIP based inter-GW mobility service. The proposal could be used by HIP-enabled UEs running any HIP-enabled or legacy network applications. The SDN-aware UFA HIP enables secure integration of untrusted non-3GPP access networks into the SDMN system, supports coexistence of IPv4 and IPv6 network segments and integrates signalling delegation based distributed UFA-HIP into SDMNs as an efficient Loc/ID splitter, security and mobility management option. In general, the proposal is a natural evolution step of UFA-HIP by:

- inheriting benefits of efficient and secure signalling delegation of UFA-HIP systems in SDMN architectures
- providing optimal UFA-GW selection based on SDN operation
- ensuring optimal path selection between source and target UFA-GW nodes during and after handover events
- efficiently supporting of different UFA-HIP deployment scenarios
- helping deployment by creating more lightweight UFA-GWs

The benefits of this use case come forward also in heterogenous access networks

- IEEE 802.21 MIH is integrated
- proactive vertical handover management is naturally supported

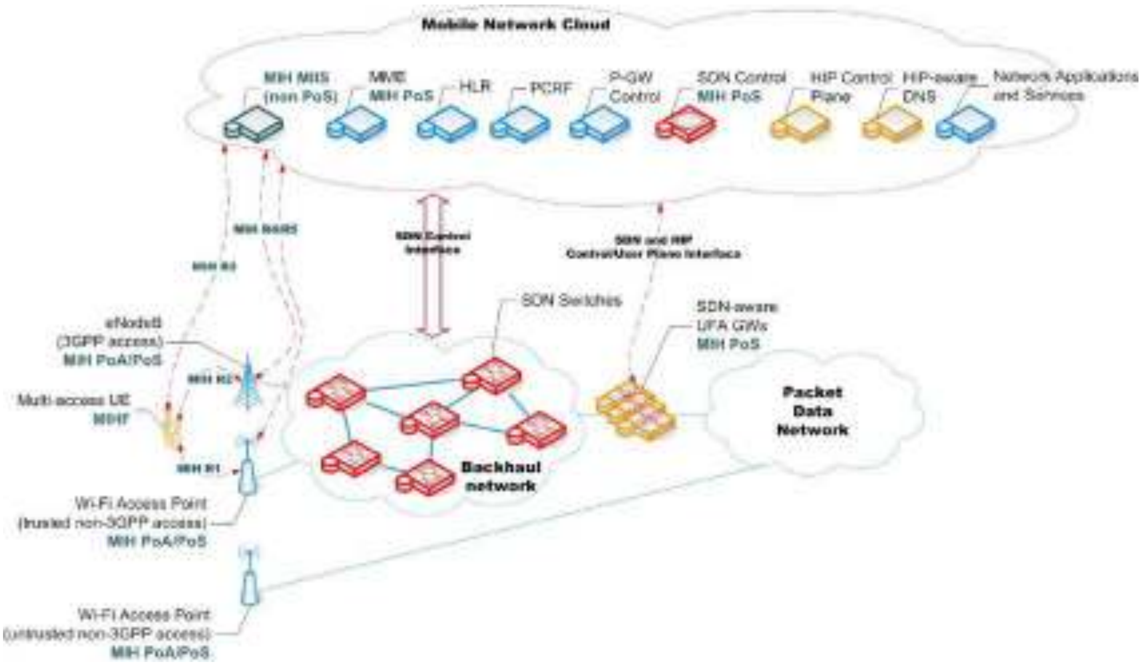

Mobile Network Cloud
MIH MIIS (non PoS)
MME MIH PoS
HLR
PCRF
P-GW Control
SDN Control MIH PoS
HIP Control Plane
HIP-aware DNS
Network Applications and Services
MIH R4/R5
MIH R3
SDN Control Interface
SDN and HIP Control/User Plane Interface
SDN Switches
SDN-aware UFA GWs MIH PoS
eNodeB (3GPP access) MIH PoA/PoS
MIH R2
Multi-access UE MIHF
MIH R1
Packet Data Network
Backhaul network
Wi-Fi Access Point (trusted non-3GPP access) MIH PoA/PoS
Wi-Fi Access Point (untrusted non-3GPP access) MIH PoA/PoS

Figure 54 – SDN-aware UFA HIP mobility management framework

5.4.2 Proxy-Mobile IPv6 in SDMNs

Our objective is to design the PMIPv6 evolution that takes full advantage of the SDN-NFV concept and to cover the challenges and objectives defined in Section 4.3.2. This use case requires an SDN southbound protocol able to provide low-level link technology information such as Received Signal Strength Indicator, wireless channel frequency, information about neighbouring wireless access-points. To that end specification of SDN software for the controller and on infrastructure devices is ongoing. Furtheremore, implementation of an NFV architecture relying on the OpenStack Cloud infrastructure is on-going as well with the necessary orchestration capabilities.

5.4.3 OpenFlow-based mobility management for heterogeneous SDMNs

The proliferation of overlapping heterogeneous access technologies, and multi-interface devices together with the current trends of increasing mobile broadband traffic volume and dynamicity motivated researches on novel networking solutions, encouraging developments in the area of mobile cloud computing, programmable network solutions and Network Function Virtualization even for multi-access environments. The technology, which provides the necessary toolset to support and widely integrate such innovative solutions, is the adaptation of the Software Defined Network paradigm into mobile Internet architectures. SDN techniques bring advanced control, configuration and management capabilities to the legacy network fabric by introducing OpenFlow-based mechanisms and operation. However there are some ongoing works regarding the application of OpenFlow in mobile networks, none of the existing SDN solutions consider link conditions and other cross-layer information when integrating OpenFlow controlling mechanisms into the handover management framework of 3GPP-based evolved mobile internet architectures. Mobility management optimization based on cross-layer information provision is crucial in the future's multi-access wireless setups when potentially a plethora of wireless technologies are simultaneously available.

Our proposal relies on the flexibility of OpenFlow-based SDN mechanisms and the cross-layer information provision and decision supporting capabilities of ANDSF and IEEE 802.21 MIH. Using OpenFlow protocol extensions, a centralized SDN controller entity controls and manages radio access links through an appropriate set of ANDSF and MIH mechanisms for obtaining access quality information, controlling link behavior, helping access network selection and supporting decisions in a flow-aware (i.e., fine grained) and access technology independent manner. With the help of OpenFlow we implement a generalized control of different access networks relying on central and network-centric optimization possibilities and offering a flexible toolset to network developers/operators for deep integration of adaptivity into the mobility management framework on the system level.

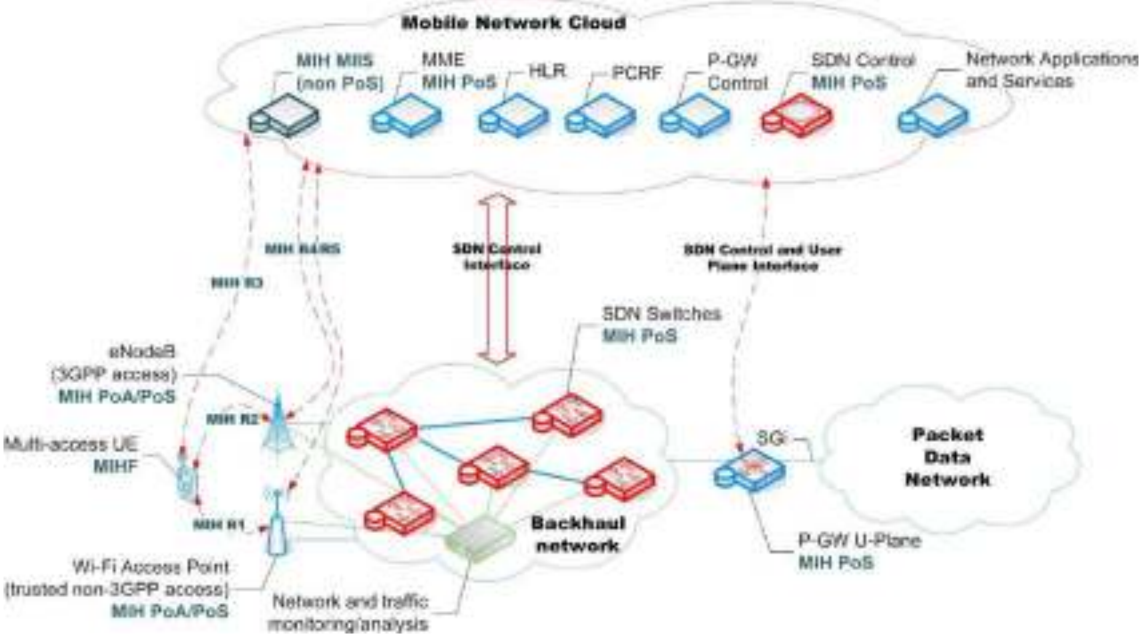


Figure 55 – SDN-based mobility management for programmable LTE/EPC architectures (IEEE 802.21+OF use-case)

In the IEEE 802.21 MIH + OF use-case we define a SDMN mobility management framework (Figure 60) and signaling scheme where MIH is used to optimize handovers among different access networks and OpenFlow configures networking nodes to proactively establish and manage communication paths for user level data flows. In this way, OpenFlow mechanisms became aware of mobility related cross-layer information and will rely on these data to select candidate access networks, optimize network resources during handover events, and configure flow paths in a proactive and highly dynamic manner according to the actual connectivity options. The impact of inter-technology handovers on the user flows can be minimized, the user and data planes can be splitted, optimal transmission routes can be continuously maintained and also flow-level decisions can be made and executed to support efficient offloading situations.

In the ANDSF + OF use-case we define an ANDSF-based SDMN mobility management framework (Figure 61) with the appropriate signaling mechanisms in order to provide intelligent access network discovery and selection during handovers in heterogeneous access environments. Using ANDSF, 3GPP compatible policy based network selection and traffic steering is achievable: deriving dynamic policies and distributing them to the ANDSF client implemented in the UEs makes SDMN operators able to initiate enhanced traffic offloading to Wi-Fi from cellular networks, ensure higher level QoS and more efficient resource utilization. Decision complexity of such flow-based vertical handover decisison arises from the fact that the network, application, and user context data and policies are available at different segments of the network (i.e., UE, RAN, backhaul, core, etc.). Therefore OpenFlow-based, centralized control scheme is to be applied in this use-case where the controller commands SDN switches to proactively modify flow tables and such manage user communication paths in the network during handover events. Extension of ANDSF mechanisms is needed because existing ANDSF standards do not take into account any dynamic network and UE conditions like load or congestion.

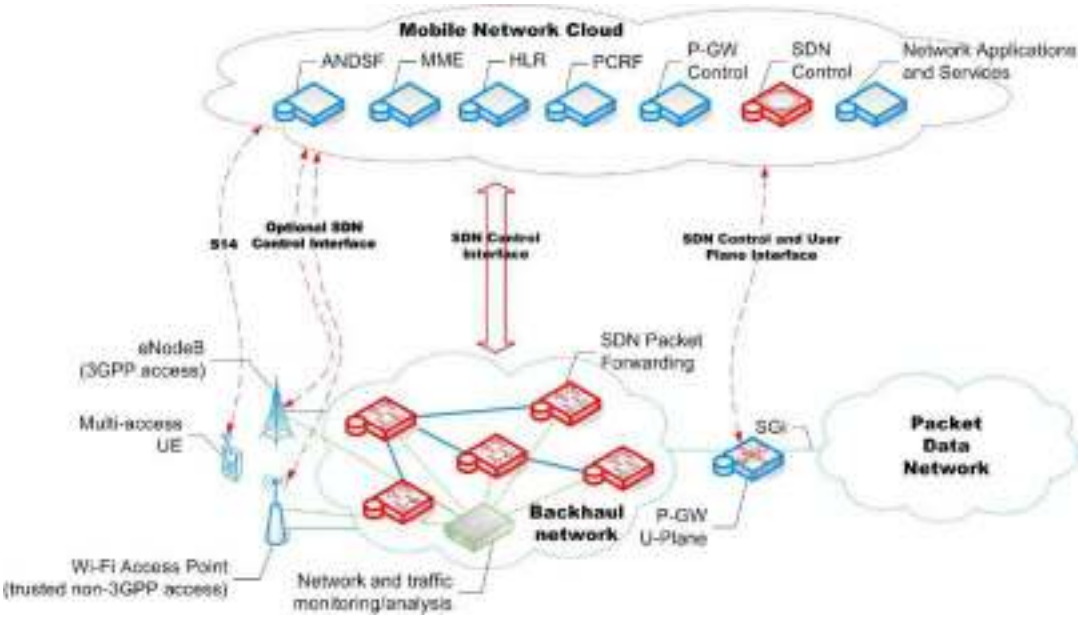


Figure 56 – SDN-based mobility management for programmable and virtualized LTE/EPC architectures (ANDSF+OF use-case)

5.4.4 Enabling secure network mobility with OpenFlow

Having a software layer controlling hardware underneath, the applications that are built on top of the software layer can be easily controlled according to the dynamic changes. Therefore, security in SDN is a piece of application that handles the potential threats and vulnerabilities. Generally, the network infrastructure, which is operating at Layer 2 and 3 is always independent from the network security operating at Layer 4 to 7 in OSI model. However, emerging SDN concepts will affect on the network across Layer 2 to 7 due to the changes in the underlying network structure which is brought about by SDN that inevitability brunt on network security. An attacker's point of view, the SDN controller is a security bottleneck due to centralized architecture.

Therefore, the interfaces to the controller must be capable of authorizing the trusted network resources based on their credentials and isolating different applications with distinct security constrains. The security objects, that are familiar with the physical domain of clouds and data centers, such as firewalls, vulnerability scanners, or access control equipments must be provided with software controlled hypervisors that speed-up the deployment and management of such networks.

These logical attributes should manage application layers and hardware to provide same security capabilities that are required in such virtualized and software defined environments. Therefore, IP address, MAC address and location information are not so important in terms of security in software defined environments, due to complicated use-cases where the workload is mobile and software networks being reconfigured or being created on the fly. Therefore, the security policies must be modified, created or removed according to the dynamic changes and topology changes of the network.

In a nutshell, the proposed OFHIP solution is an integration of diet version of HIP layer with the existing OpenFlow version to replace the SSL/TLS based mutual authentication. As a result, we would get almost the same level of security with enhanced mobility support.

It provides end-to-end encryption, mutual authentication and secure key exchange. The HIP layer identifies a host either by a host identifier (HI) or a host identity tag (HIT). HI is the public key of an asymmetric key-pair which could be used as a local identity. However, it is not suitable to serve as a packet identifier, since the length can vary.

Mutual authentication in OpenFlow is a part of security assertion, which is achieved with SSL or TLS. They operate at the transport layer in the OSI stack, and provide secured data transport for applications. It supports peer negotiation for algorithm selection, public key-based exchange of secret session keys and X.509 certificates. However, they do not support mobility alone without the support of an underlying protocol (UDP, SCTP and etc). The modified version of TLS; DTLS can be used by applications directly or by tunnelling to provide secure mobility.

However, with legacy IP protocols, the handover impact at the upper layers is still tight. OFHIP proposal described in Figure 57. OFHIP solution atchitecture for sealmess and secure mobilityuses IPSec encapsulating security payload (ESP) secure associations (SAs) that are bound to HITs. Therefore, address reconfiguration would not have any impact on the higher-layer associations except the changes in network routing layer.

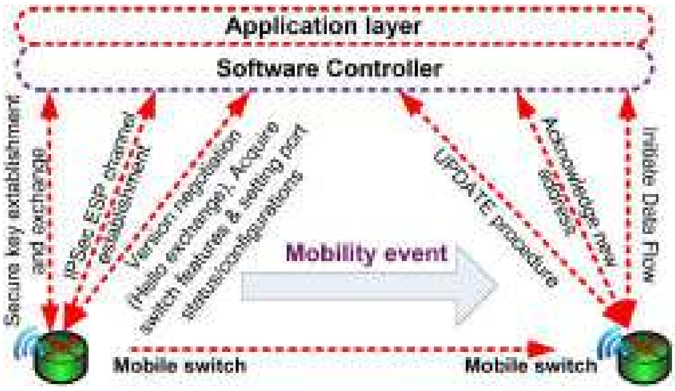

Application layer
Software Controller
Secure key establishment and exchange
IPSec ESP channel establishment
Version negotiation (Hello exchange), Acquire switch features & setting port status/configurations
Mobility event
UPDATE procedure
Acknowledge new address
Initiate Data Flow
Mobile switch
Mobile switch

Figure 57. OFHIP solution atchitecture for sealmess and secure mobility.

The key-exchange in OFHIP is a cryptographic protocol that uses a randomly generated key encrypted by a Diffie-Hellman derived key in order to establish a pair of IPsec-ESP SAs between two entities; the initiator and the responder. The HIP layer in OFHIP solution maps arriving ESP packets to a HIT using the security parameter index (SPI) value in the packet and selects the source address and interface according to the SPI value set by ESP.

After handover, data continues to flow inside of the ESP tunnel with the same SPI values but with a different IP address at the mobile node. The initiator defines SPI value of the responder’s outgoing SA, whereas the responder defines the SPI value of the initiators outgoing SA. To prevent replay attacks, we propose to use an incremental counter with a hash of the HIT.

For secure mobility, rekeying may be necessary. Thus, new SAs must be created by removing the old SAs. Once a host receives data on new SA, it can safely remove the old SA. The HIP layer uses AES-CBC for symmetric encryption and to provide CMAC for MACing functions while the session keys are encrypted with elliptic curve diffie-hellman (ECDH) keys.

Four-packet exchange makes OFHIP resilient to denial-ofservice (DoS). The protocol transmits an EC Diffie-Hellman encrypted key in the 3rd and 4th packets, and authenticates the parties with those packets. The responder starts a puzzle exchange with the initiator in the 2nd packet, and completes it in the 3rd packet before the responder stores any state from the exchange. This model falls in the line of TLS and fairly equivalent to 802.11 master and pair-wise transient key, but handled in a single exchange.

6. Conclusions

In this document we surveyed the state-of-the-art (Chapter 2) and the relevant standardization activites (Chapter 3) related to resource, traffic and mobility management in virtualized and software defined mobile architectures. We collected different research topics in the field, and defined the main expected benefits and challenges to be tackled under those topics (Chapter 4). Finally, we proposed use cases, which will highlight the results of our work (Chapter 5).

The following research topics have been defined.

1) **Resource management (RM)**

- Resource availability awareness in SDMNs

  The integration of SDN and NFV into LTE, allows incremental updates of network elements provided by different vendors as well as virtualized network functions providers. Heterogeneity of resources and dynamicity of them are a challenge for network configuration awareness by means of availability of resources. Both physical and virtualized resource operators require to have updated information on available inventory, topology, capacity, resilience and optionally security assurance assessment. In any case resource availability awareness is the foundation for resource management process, service provisioning and optimization, traffic management as well as security protection and monitoring process. Awareness of resource availability may be filtered in different views for VMNOs vs centralized global unique MNO.

- Optimized video delivery

  Video Service Providers should be able to select the most adequate data center for video delivery. The objectives are resource localization, resource availability monitoring, management of network bandwidth, and media delivery. The objective is to enable E2E traffic optimization from client to cloud applications. Traffic path is driven by the applications that can guaranty a Service Level Agreement.

- In-network caching

  In-network caching allows storing the content in a location close to the users, caching permits to reduce the load on the network. The in-network caching allows to move the cache trought the network. This enables that contents are served from a location close to the users, thus the packets travel less, so the network resources are spared. Caching mainly avoids that requests to the same contents go every time through the whole network to the packet gateways and the interconnections

2) **Macroscopic-level traffic management**

- Joint traffic and cloud resource management for service chaining in SDMNs

  Traffic management in modern mobile networks is much more than simply establishing a connection between two end points. Control functionalities in these networks typically include firewall, deep-packet inspection, carrier-grade NAT, IPS/IDS, etc. While establishing a flow connection, the SDMN controller should make sure that these functionalities are included as part of the route in a specified order as a service chain. Furthermore, with the proliferation of cloud technologies, the majority of these functionalities are now being realized in the VMs in the cloud. Such a distributed realization of these functionalities will no doubt require continuous updating of the VM locations in real time as a result of user mobility as well as load balancing. In this research, joint dynamic routing and service VM selection algorithms will be established to run as a “Service Chaining” application on the SDMN controller with targets like delay minimization, congestion minimization etc.

- Coordinated traffic and resource management and efficient routing in SDMNs

  The impacts of software defined mobile networking on traffic and resource management will be analysed and efficient routing algorithms to be optimized based on the individual service needs (for different QoS and/or QoE requirements) will be developed by exploiting the benefits of the software defined mobile networking paradigm. Dynamic traffic and resource allocation algorithms to provide input to the network virtualization will be examined. Possibilities of energy efficient routing will be investigated.

- Application-level traffic optimization in SDMNs

  Integration of application layer traffic optimization (ALTO) in software-defined mobile networks could have several benefits for orchestration of endpoint selection for distributed services. ALTO can provide guidance, e.g., in the redirection of end users to appropriate in-network cache, content distribution network server or virtual network function instance during service chaining.

ALTO service provides appropriate level of abstraction of network and cost maps, enforcing the policies of mobile network operator and optionally other actors, but keeping the privacy of network topology information. SDN controllers can enforce flow redirection and can dynamically provide abstracted network and cost maps to ALTO server.

- SDN-controlled IP Wireless Mesh Network for 3GPP RAN offloading

  This research topic addresses the opportunity of offloading the Radio Access Network by the use of IP Wireless Mesh Network (e.g. WiFi). Here we consider SDN control of IP communications in the edge networks, meaning that smartphones are SDN capable. It is commonly assumed that such a target would be handled by end-terminals themselves as a completely distributed system without mobile network supervision. This research topic investigates wether the mobile network operator can keep control of these communications to redirect traffic to a different access network.

3) Microscopic-level traffic management

- DiffServ QoS in SDN-based transport and policy control in SDMNs

  DiffServ QoS architecture can provide soft QoS guarantees on top of different Layer-2 technologies in a scalable manner. However, in current SDN standards (e.g., OpenFlow, OpenFlow Configuration) QoS management is still in early stage. Our research will focus on dynamic provision of QoS rules in network forwarding paths of MNOs and VMNOs

- QoS/QoE enforcement in SDMNs

  The QoE Managaement framework ISAAR can benefit from adding SDN functionalities. The quality monitoring of Internet services starts with identification of the respected flows within the traffic mix. Normally a lot of processing is needed for this detection, due to the Deep Package Inspection (DPI) required. To simplify that mechanism the OpenFlow (OF) matching rules can be used. Therefore, the OF controller has to be configured in a way which allows identifying measurable traffic by using the matching rules and teeing it out to one of the measuring points of ISAAR in real-time. This flow selective copy port mechanism allows for traffic steering of the relevant packets towards centralized measurement probes. On the other hand OF functionalities can be used for changing the per hop behaviour (PHB) for each traffic flow.

4) Mobility management

- Extension of legacy solutions for mobility management in SDMNs

  In the field of mobility management the following research questions are investigated. Current 3GPP networks make use of mobility management protocols, which are based on different IP tunnelling options (MIP, PMIP, GTP). The main research questions are the integration of centralized and/or distributed anchors with the SDN forwarding functions, host-based mobility management where the mobile node also deals with encapsulation/decapsulation duties, QoS/QoE driven mobility management and support of complex mobility scenarios (e.g., network mobility, flow mobility, macro- and micro-mobility, session mobility) in Software-Defined Mobile Networks.

- Proxy Mobile IPv6 integrated into SDN/NFV ecosystem

  This research topic investigates the integration of Proxy Mobile IPv6 into SDN/NFV architecture. Important challenges are, e.g., integration with service chaining, coordination with the orchestrator, handling of the SDN control plane, emulation of network functions (Mobile Access Gateway – MAG, Local Mobility Anchor - LMA), and relocation of the LMA function on a per user basis.

- SDN based extensions to LTE/EPC mobility management

  We are also concerned with purely SDN-based mobility management solutions. The advantages of such solutions are that mobility transparency can be provided to higher layers even without applying additional tunnelling. However, it is challenging, how complex mobility scenarios and additional features will be realized, such as identity-locator splitting or routing protocol independency of different network domains, which are already supported by current distributed mobility management solutions.

- Enabling secure network mobility with OpenFlow

  OpenFlow at the current stage does not support mobility. This is a critical downfall that limits OpenFlow into fixed core-networks, clusters or data centers. Robust multipath connectivity for fault tolerance is one of the critical issue inhabits in the current SDN architecture. This is even more crucial when the controller or the switch is mobile. In one hand, multiple channels between the switch and the controller can guarantee a certain level of assurance for seamless connectivity. Mobile base stations, mobile routers, switchers, mobile clouds and server migration are some of the compelling reasons why mobility is insisted in SDNs. This would extend SDN benefits into mobile environments e.g., moving trains, buses, flights and other automobiles.

References

[1] NMHH, „Current Issues of Net Neutrality, Preparatory Document for Public Consultation", May 2012, URL: http://nmhh.hu/dokumentum/150627/network_neutrality_consultation_document.pdf

[2] D. Sun, Ed., H. Tschofenig, T. Tsou, A. Doria, G. Zorn, Ed., "Diameter Quality-of-Service Application", IETF, RFC 5866, May 2010.

[3] 3GPP, "Policy and charging control architecture (Release 12)", TS 23.203, v12.2.0, September 2013.

[4] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 12)", TS 23.401, v12.2.0, September 2013.

[5] 3GPP, "Architecture enhancements for non-3GPP accesses (Release 12)", TS 23.402, v12.2.0, September 2013.

[6] K. Ramakrishan, S. Floyd, D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", IETF, RFC 3168, September 2001.

[7] Open Networking Foundation, "OpenFlow Switch Specification", version 1.3.2, April 25, 2013.

[8] Open Networking Foundation, "OpenFlow Management and Configuration Protocol (OF-Config 1.1.1)", version 1.1.1, March 23, 2013.

[9] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services", IETF, RFC 2475, December 1998.

[10] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", IETF, RFC 2474, December 1998.

[11] J. Heinanen, Telia Finland, F. Baker, W. Weiss, J. Wroclawski, "Assured Forwarding PHB Group", IETF, RFC 2597, June 1999.

[12] V. Jacobson, K. Nichols, K. Poduri, "An Expedited Forwarding PHB", IETF, RFC 2598, June 1999.

[13] "Differentiated Service on Linux HOWTO", URL: http://www.softwareopal.com/qos/default.php?p=linux101-ds , October 2013.

[14] "Differentiated Service on Cisco HOWTO", URL: http://www.softwareopal.com/qos/default.php?p=cisco102-cds, October 2013.

[15] Santiago Álvarez, "QoS in MPLS Networks", RST 1607, Networkers 2004.

[16] J. Seedorf, E. Burger, „Application-Layer Traffic Optimization (ALTO) Problem Statement", IETF, RFC 5692, October 2009.

[17] M. Stiemerling, S. Kiesel, S. Previdi, Alcatel-Lucent Bell Labs, "ALTO Deployment Considerations", IETF, draft-ietf-alto-deployments-07, July 15, 2013.

[18] Young Lee, Greg Bernstein, Sreekanthm, Dhruv Dhody, Taesang Choi, "ALTO Extensions for Collecting Data Center Resource Information", IETF, draft-lee-alto-ext-dc-resource-02, July 8, 2013.

[19] H. Xie, T. Tsou, D. Lopez, H. Yin, "Use Cases for ALTO with Software Defined Networks", IETF, draft-xie-alto-sdn-use-cases-01, June 27, 2012.

[20] S. Kiesel, Ed., S. Previdi, M. Stiemerling, R. Woundy, Y. Yang, "Application-Layer Traffic Optimization (ALTO) Requirements", IETF RFC 6708, September 2012.

[21] R. Alimi, Ed., Y. Yang, Ed., et al., "Application-Layer Traffic Optimization (ALTO) Protocol", IETF RFC 7285, September, 2014.

[22] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", IETF, RFC 2616, June 1999.

[23] Perkins, C. et al.: Mobility Support in IPv6. IETF RFC 6275 (2011).

[24] Koodli, R.: Fast Handovers for Mobile IPv6. IETF RFC 4068 (2005).

[25] Soliman, H. et al.: Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. IETF RFC 5380 (2008).

[26] R. Wakikawa (Ed.), V. Devarapalli, G. Tsirtsis, T. Ernst, K. Nagami: Multiple Care-of Addresses Registration, IETF RFC 5648, October 2009.

[27] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert: Network Mobility (NEMO) Basic Support Protocol, IETF RFC 3963, Jan. 2005.

[28] H. Soliman (Ed.), Mobile IPv6 Support for Dual Stack Hosts and Routers, IETF RFC 5555, June 2009.

[29] S. Gundavelli (Ed.), K. Leung, V. Devarapalli, K. Chowdhury, B. Patil: Proxy Mobile IPv6, IETF RFC 5213, Aug. 2008.

[30] Valko: Cellular IP: A New Approach to Internet Host Mobility, ACM SIGCOMM Comp. Commun. Rev., 29 (1), 50-65., 1999.

[31] R. Ramjee, T. L. Porta, S. Thuel, K. Varadhan, S. Wang, HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-area Wireless Networks. IEEE Int. Conf. Network Protocols, 1999.

[32] Grilo, P. Estrela, M. Nunes: Terminal Independent Mobility for IP (TIMIP). IEEE Communications Magazine , 34-41., 2001.

[33] T. Melia, A. de la Oliva, A. Vidal, I. Soto, D.; Corujo, R. L. Aguiar, Toward IP converged heterogeneous mobility: A network controlled approach. In Com. Networks, vol. 51. 2007.

[34] IEEE, IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover, IEEE Std 802.21-2008, Jan. 2009.

[35] 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses, Rel.10,V10.2, 2011.

[36] 3GPP TS 29.275, Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunneling protocols, Stage 3, Release 10, V10.0.0, Dec. 2010.

[37] 3GPP TS 24.303, Mobility management based on Dual-Stack Mobile IPv6, Stage 3, Release 10, V10.1.0 Dec. 2010.

[38] 3GPP TS 23.261. (September 2010). IP flow mobility and seamless Wireless Local Area Network (WLAN) offload, Stage 2, Release 10. 3GPP Technical Specification.

[39] 3GPP TS 23.402. (June, 2011). Architecture enhancements for non-3GPP accesses, Release 10, V10.4.0. 3GPP Technical Specification.

[40] 3GPP TR 23.829. (Sept. 2010). Local IP Access and Selected IP Traffic Offload, Release 10, V1.3.0. 3GPP Technical Report.

[41] 3GPP TS 23.401 V10.4.0. (June 2011). General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, Release 10. 3GPP Technical Specification.

[42] P. Thubert, R. Wakikawa, V. Devarapalli: Global HA to HA protocol, IETF Internet-Draft, draft-thubert-nemo-global-haha-02.txt, Sept. 2006.

[43] M. Fischer, F.-U. Andersen, A. Kopsel, G. Schafer, M. Schlager: A Distributed IP Mobility Approach for 3G SAE, In Proc. of 19th PIMRC, ISBN: 978-1-4244-2643-0, Sept. 2008.

[44] R. Farha, K. Khavari, N. Abji, A. Leon-Garcia: Peer-to-peer mobility management for all-ip networks, In Proc. of ICC ’06, V. 5, pp. 1946–1952, June 2006.

[45] M. Bauer, P. Bosch, N. Khrais, L. G. Samuel, P. Schefczik: The UMTS base station router, Bell Labs Tech. Journal, I.: Wireless Network Technology, V. 11, I. 4, pp. 93–111, 2007.

[46] Liu Yu, Zhao Zhijun, Lin Tao, Tang Hui: Distributed mobility management based on flat network architecture, In Proc. of 5th WICON, pp. 1-5, Singapore, 2010.

[47] R. Moskowitz, P. Nikander, P. Jokela (Ed.), T. Henderson: Host Identity Protocol, IETF RFC 5201, April 2008.

[48] A.C. Snoeren, H. Balakrishnan: An End-to-End Approach to Host Mobility, In Proc. of MobiCom, Aug. 2000.

[49] D. Maltz, P. Bhagwat, MSOCKS: An Architecture for Transport Layer Mobility, In Proc. INFOCOM, pp. 1037-1045, Mar. 1998.

[50] R. Stewart (Ed.): Stream Control Transmission Protocol, IETF RFC 4960, Sept. 2007.

[51] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler: SIP: Session Initiation Protocol, IETF RFC 3261, June 2002.

[52] Z. Faigl, L. Bokor, P. Neves, K. Daoud, P. Herbelin, Evaluation of two integrated signalling schemes for the ultra flat architecture using SIP, IEEE 802.21, and HIP/PMIP protocols, In journal of Computer Networks, doi:10.1016/j.comnet.2011.02.005, 2011.

[53] L. Bokor, Z. Faigl, S. Imre, A Delegation-based HIP Signaling Scheme for the Ultra Flat Architecture, In Proc. of the 2nd IWSCN, pp. 9–16., Karlstad, Sweden, 2010.

[54] P. Bertin, S. Bonjour, J.-M. Bonnin, A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures, In Proc. of NTMS '08, pp.1-5, 2008.

[55] P. Bertin, S. Bonjour, J. Bonnin, Distributed or centralized mobility?, In Proc. of the 28th IEEE conference on Global telecommunications (GLOBECOM’09), Honolulu, HI, 2009.

[56] M. Kassi-Lahlou, C. Jacquenet, L. Beloeil, X. Brouckaert, Dynamic Mobile IP (DMI), IETF Internet-Draft, draft-kassi-mobileip-dmi-01.txt, Jan. 2003.

[57] M. Song, J. Huang, R. Feng, J. Song, A Distributed Dynamic Mobility Management Strategy for Mobile IP Networks, In Proc. of 6th ITST, pp. 1045-1050, June 2006.

[58] P. Seite, P. Bertin, Dynamic Mobility Anchoring, IETF Internet-Draft, May 2010.

[59] Z. Yan, L. Lei, M. Chen, WIISE - A Completely Flat and Distributed Architecture for Future Wireless Communication Systems, Wireless World Research Forum, Oct. 2008.

[60] Gurtov et al., Hi3: An efficient and secure networking architecture for mobile hosts, Journal of Computer Communications, vol. 31, no. 10, pp. 2457–2467, 2008.

[61] Network Functions Virtualisation, White Paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

[62] S. Matsushima, R. Wakikawa, Stateless user-plane architecture for virtualized EPC (vEPC), IETF I-D, draft-matsushima-stateless-uplane-vepc-01, 2013.

[63] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., & Patil, B. (2008. August). Proxy Mobile IPv6. IETF RFC 5213.

[64] Soliman, H. (. (2009. June). Mobile IPv6 Support for Dual Stack Hosts and Routers. IETF RFC 5555.

[65] R. Wakikawa, R. Pazhyannur, S. Gundavelli, Separation of Control and User Plane for Proxy Mobile IPv6, IETF I-D, draft-wakikawa-netext-pmip-cp-up-separation-00.txt, 2013.

[66] Andrew L. Dul, Global IP Network Mobility using Border Gateway Protocol (BGP), IAB Plenary IAB Plenary of IETF, 62nd, March 2005.

[67] Zhu, Z., Wakikawa, R., and L. Zhang, A Survey of Mobility Support in the Internet, RFC 6301, July 2011.

[68] Stateless user-plane architecture for virtualized EPC (vEPC), Presentation on IETF 87, http://www.ietf.org/proceedings/87/slides/slides-87-dmm-5.pdf

[69] B. Sarikaya, Mobility Management Protocols for Cloud-Like Architectures, IETF I-D, draft-sarikaya-dmm-cloud-mm-00.txt, 2012.

[70] Mobility Management Protocols for Cloud-Like Architectures, Presentation on IETF 85, http://tools.ietf.org/agenda/85/slides/slides-85-dmm-6.pdf

[71] Perkins, C., "Alternate Tunnel Source Address for LMA and Home Agent", IETF I-D, draft-perkins-netext-hatunaddr-00, 2012.

[72] Kovács, J., Bokor, L., Kanizsai, Z., & Imre, S., Review of Advanced Mobility Solutions for Multimedia Networking in IPv6. In D. Kanellopoulos (Ed.), Intelligent Multimedia Technologies for Networking Applications: Techniques and Tools (pp. 25-47), 2013.

[73] H. Anthony Chan, Hidetoshi Yokota. Jiang Xie, Pierrick Seite, Dapeng Liu Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues JOURNAL OF COMMUNICATIONS, VOL. 6, NO. 1, FEBRUARY 2011

[74] CJ. Bernardos, A. de la Oliva, F. Giust, An IPv6 Distributed Client Mobility Management approach using existing mechanisms, IETF I-D, draft-bernardos-mext-dmm-cmip-00, 2011.

[75] K. Yap, R. Sherwood, M. Kobayashi, T. Huang, M. Chan, N. Handigol, N. McKeown, and G. Parulkar. Blueprint for introducing innovation into wireless mobile networks. In Proceedings of the second ACM SIGCOMM workshop on Virtualized infrastructure systems and architectures, pages 25-32. ACM, 2010.

[76] A. Coyle and H. Nguyen. A frequency control algorithm for a mobile adhoc network. In Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, November 2010.

[77] P. Dely, A. Kassler, and N. Bayer. OpenFlow for wireless mesh networks. In Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), pages 1-6. IEEE, 2011.

[78] Pentikousis, K.; Yan Wang; Weihua Hu, "Mobileflow: Toward software-defined mobile networks," Communications Magazine, IEEE , vol.51, no.7, pp.44,53, July 2013.

[79] Peter Dely, Andreas Kassler, Lawrence Chow, Nicholas Bambos, Nico Bayer, Hans Einsiedler, Christoph Peylo, Daniel Mellado, Miguel Sanchez, A software-defined networking approach for handover management with real-time video in WLANs, Journal of Modern Tansportation, Volume 21, Issue 1, pp 58-65, 2013.

[80] S. Agarwal, M. Kodialam, and T. V. Lakshman, “Traffic engineering in software defined networks" In Proc. IEEE INFOCOM, pp. 2211-2219, 2013.

[81] Z. Arslan, A. Alemdaroglu and B. Canberk, “A Traffic-Aware Controller Design for Next Generation Software Defined Networks”, International Black Sea Conference on Communications and Networking (BlackSeaCom), pp.167-171, 2013.

[82] W-C. Liao, M. Hong, H. Farmanbar, X. Li, Z-Q. Luo, and H. Zhang, “Min Flow Rate Maximization for Software Defined Radio Access Networks”, Submitted to JSAC special issue on 5G Wireless Communication Systems, December 2013.

[83] A. Chanda, C. Westphal, and D. Raychaudhuri, “Content based traffic engineering in software defined information centric networks,” in inProc. IEEE INFOCOM workshop NOMEN’13, Apr. 2013, pp. 1-6.

[84] X. Jin, L.-E. Li, V. Laurent, and R. Jennifer, “Cellsdn: Software-defined cellular core networks,” in open net summit, 2013.

[85] X. Jin, L. E. Li, L. Vanbever, and J. Rexford, “ SoftCell: Taking control of cellular core networks," Tech. Rep. TR-95-13, Princeton University CS, May 2013.

[86] F. Esposito, I. Matta and V. Ishakian, “Slice Embedding Solutions for Distributed Service Architectures”, ACM Computing Surveys, Vol. 46, Bo. 1, Article 6, October 2013.

[87] J. He at al., “DaVinci: Dynamically adaptive virtual networks for a customized internet”, in the Proceedings of the ACM CoNEXT Conference (CoNEXT’08), 2008.

[88] J. Londono, A. Bestavros, S. Teng, Collocation games and their application to distributed resource management. In the Proceedings of the USENIX Workshop on Hot Topics in Cloud Computing (HotCloud’09).

[89] J.Lu and J. Turner, “Efficient mapping of virtual networks onto a shared substrate”, Tech. rep., Washington University in St. Louis, http://www.arl.wustl.edu/Publications/2005-09/wucs2006-35.pdf, 2006.

[90] M. Yu et al.,”Rethinking virtual network embedding: Substrate support for path splitting and migration”, SIGCOMM Comput. Comm. Rev. 38, 2, 17-29, 2008.

[91] J. Fan, M. Ammar, “Dynamic topology configuration in service overlay networks: A study of reconfiguration policies”, In Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM’06), 2006.

[92] Organization for the Advancement of Structured Information Standards (OASIS), Universal description, discovery and integration. Version 3.0.2. http://www.oasis-open.org/standards , 2006.

[93] RSP: http://www.protogeni.net/trac/protogeni/wiki/RSpec, 2013.

[94] Y. Zhu et al., “Cabernet: Connectivity architecture for better network services,” in Proceedings of the ACM CoNEXT Conference (CoNEXT’08). ACM Press, New York, 64:1-64:6, 2008

[95] I. Houidi et al., “Virtual network provisioning across multiple substrate networks,” Computer Networks, 55, 4, 1011-1023, 2011.

[96] I. Houidi et al., “A distributed virtual network mapping algorithm, ” in Proceedings of the IEEE International Conference on Communications (ICC’08), 5634-5640, 2008.

[97] M. Chowdhury et al. “PolyVine: Policy-based virtual network embedding across multiple domains, ” in Proceedings of the ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architecture (VISA’10), ACM Press, New York, 49-56, 2010.

[98] F. Esposito et al., “A generally distributed approach to slice embedding with guarantees, ” Tech. Rep. TR2012-014, Boston University.

[99] Dan C. Marinescu, Cloud Computing: Theory and Practice, Morgan Kaufmann, Elsevier Inc., ISBN: 978-0-12404-627-6, 2012.

[100] R. R. Sambasivan, A. X. Zheng, M. De Rosa, E. Krevat, S. Whitman, M. Stroucken, W. Wang,L. Xy, and G. R. Ganger. “Diagnosing performance changes by comparing request flows.” Proc. 8th USENIX Conf. on Networked SystemsDesign and Implementation (NSDI’11), pps. 14, 2011.

[101] F. Chang, J. Ren, and R. Viswanathan. “Optimal resource allocation in clouds.” Proc. IEEE 3rd Int. Conf. on Cloud Computing, pp. 418–425, 2010.

[102] R. Aoun, E. A. Doumith, and M. Gagnaire. “Resource provisioning for enriched services in cloud environment.” Proc. IEEE 2nd Int. Conf. on Cloud Computing Technology and Science, pp. 296–303, 2010.

[103] B. Abrahao, V. Almeida, J. Almeida, A. Zhang, D.Beyer, and F. Safai. “Self-adaptive SLA-driven capacity management for Internet services.” Proc. IEEE/IFIP Network Operations & Management Symposium (NOMS06), pp. 557–568, 2006.

[104] D. Ardagna, M. Trubian, and L. Zhang. “SLA based resource allocation policies in autonomic environments.” J. Parallel Distrib. Comp., 67(3):259–270, 2007.

[105] K. Boloor, R. Chirkova, Y. Viniotis, and T. Salo. “Dynamic request allocation and scheduling for context aware applications subject to a percentille response time SLA in a distributed cloud.” Proc. IEEE 2nd Int. Conf. on Cloud Computing Technology and Science, pp. 464–472, 2010.

[106] J. Medved et al., „ALTO Network-Server and Server-Server APIs”, http://tools.ietf.org/id/draft-medved-alto-svr-apis-00.txt

[107] P. Racz, Z. Despotovic, „An ALTO Service based on BGP Routing Information”, http://tools.ietf.org/id/draft-racz-bgp-based-alto-service-00.txt

[108] H. Gredler, J. Medved, S. Previdi, A. Farrel, S. Ray, „North-Bound Distribution of Link-State and TE Information using BGP”, http://tools.ietf.org/html/draft-ietf-idr-ls-distribution-04

[109] T. Bates, R. Chandra, D. Katz, Y. Rekhter, Multiprotocol Extensions for BGP-4, http://tools.ietf.org/html/rfc4760

[110] Y. Lee, G. Bernstein, Grotto Networking, D. Dhody, T. Choi, "ALTO Extensions for Collecting Data Center Resource Information", http://tools.ietf.org/id/draft-lee-alto-ext-dc-resource-03.txt

[111] Gautam Khetrapal, Saurabh Kumar Sharma, “Demystifying routing services in software-defined networking,” Aricent, Whitepaper, 2013.

[112] J. L. Deng. Introduction to grey system theory. J. Grey Syst., 1(1):1–24, November 1989.

[113] A. Huszak and S. Imre. Eliminating Rank Reversal Phenomenon in GRA-Based Network Selection Method. In Proceedings of IEEE International Conference on Communications (ICC), 2010, pages 1–6, Cape Town, South Africa, 23-27May 2010.

[114] F.A. Lootsma. Multi-criteria decision analysis via ratio and difference judgement, volume 29 of Applied Optimization. Kluwer Academic, Dordrecht, 1999.

[115] E. Triantaphyllou and K. Baig. The impact of aggregating benefit and cost criteria in four MCDA methods. IEEE Transactions on Engineering Management, 52(2):213–226, May 2005.

[116] Phuoc Nguyen Tran and Nadia Boukhatem. The distance to the ideal alternative (DiA) algorithm for interface selection in heterogeneous wireless networks. In Proc. of the 6th ACM Int. Symp. on Mobility management and wireless access 2008 MobiWac ’08, pages 61–68, Oct. 2008.

[117] R.Venkata Rao. Improved multiple attribute decision making methods. In Decision Making in Manufacturing Environment Using Graph Theory and Fuzzy Multiple Attribute Decision Making Methods, Springer Series in Advanced Manufacturing, pages 7–39. Springer London, 2013.

[118] T. L. Saaty. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. McGraw-Hill, New York, St. Louis, San Francisco, 1980.

[119] Ying-Ming Wang and Ying Luo. On rank reversal in decision analysis. Mathematical and Computer Modelling, 49(5–6):1221–1229, 2009.

[120] Jonathan Barzilai and Boaz Golany. AHP rank reversal, normalization and aggregation rules. Infor-Information Systems and Operational Research, 32(2):57–64, 1994.

[121] P. TalebiFard and V.C.M. Leung. A dynamic context-aware access network selection for handover in heterogeneous network environments. In Proc. of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 385 –390, April 2011.

[122] Q. Song and A. Jamalipour. A network selection mechanism for next eneration networks. In Proc. of the 2005 IEEE International Conference on Communications (ICC 2005), volume 2, pages 1418–1422 Vol. 2, may 2005.

[123] F. Bari and V. Leung. Multi-Attribute Network Selection by Iterative TOPSIS for Heterogeneous Wireless Access. In Proc of the 4th IEEE Consumer Communications and Networking Conference, 2007 (CCNC 2007), pages 808–812, January 2007.

[124] C. T. R. Hager. Context Aware and Adaptive Security for Wireless Networks. PhD thesis, Virginia Polytechnic Institute and State University, November 2004.

[125] H. Johnson. Toward Adjustable Lightweight Authentication for Network Access Control. PhD thesis, Blekinge Institute of Technology, Ronneby, Sweden, December 2005.

[126] B. S. Ghahfarokhi and N. Movahhedinia. Context-Aware Handover Decision in an Enhanced Media Independent Handover Framework. Wireless Personal Communications, 68:1633–1671, February 2013.

[127] K. Bala M. K. and B.R. Tamma. An enhanced media independent handover framework for heterogeneous wireless networks. In Proc. of the 12th International Conference on Intelligent Systems Design and Applications (ISDA), 2012, pages 610–615, November 2012.

[128] M. Stiemerling, S. Kiesel, S. Previdi, and M. Scharf. ALTO Deployment Considerations. IETF Draft, draft-ietf-alto-deployments-08, October 2013.

[129] Zoltán Faigl, László Bokor, “Validation and demonstration plan”, VirtMobOpt D5.1, April 2014.

[130] ITU-T G.114 One-way transmission time http://www.itu.int/rec/T-REC-G.114-200305-I/en

[131] SDN and ALTO integration, IETF draft at http://www.internetsociety.org/articles/software-defined-networking-efforts-debuted-ietf-84

[132] U.S. Federal Communications Commission: Unofficial announcement of Commission action. [online] [Accessed on 11 May 2011] at http://www.telecomlawmonitor.com/uploads/file/NN%20Public%20Notice.pdf.

[133] NMHH, „Current Issues of Net Neutrality, Preparatory Document for Public Consultation”, May 2012, URL: http://nmhh.hu/dokumentum/150627/network_neutrality_consultation_document.pdf

[134] K. Daoud, P. Herbelin, and N. Crespi. UFA: Ultra Flat Architecture for high bitrate services in mobile networks. In Proceedings of the IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC’08, pages 1–6, Cannes, France, September, 15–18, 2008.

[135] Daoud, Khadija, Guillouard, Karine, Herbelin, Philippe and Crespi, Noël. "A Network-Controlled Architecture for SCTP Hard Handover." VTC Fall, 2010.

[136] 3GPP. Security Aspects of non-3GPP Accesses (Release 11). TS 33.402, March 2012.

[137] Fabien Allard and Jean-Marie Bonnin. An application of the context transfer protocol: IPsec in a IPv6 mobility environment. International Journal of Communication Networks and Distributed Systems, 1(1):110–126, 2008.

[138] Fabien Allard et al. IKE context transfer in an IPv6 mobility environment. In Proceedings of the 3rd international workshop on Mobility in the evolving internet Architecture (MobiArch ’08), pages 55–60, Aug. 22, 2008.

[139] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli. Context Transfer Protocol (CXTP). RFC 4067, July 2005.

[140] P. Nikander and J. Arkko. Delegation of Signalling Rights. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, Security Protocols, volume 2845 of Lecture Notes in Computer Science, pages 575–586. Springer, 2004.

[141] S. Herborn, A. Huber, R. Boreli, and A. Seneviratne. Secure Host Identity Delegation for Mobility. In Proceedings of the 2nd International Conference on Communication Systems Software and Middleware (COMSWARE ’07), pages 1–9, Bangalore, India, Jan. 7–12, 2007.

[142] Werner Almesberger. TCP Connection Passing. In Proceedings of the Linux Symposium, Volume One, pages 1–13, Ottawa, Canada, Jul. 21–24, 2004.

[143] R. Farahbakhsh and N.Movahhedinia. Using context transfer mechanisms to Improve Mobile IMS-IPv6 Handover Latency and QoS provisioning. In Proceedings of the 2nd International Conference on Internet Multimedia Services Architecture and Applications (IMSAA ’08), pages 1–6, Bangalore, India, Dec 2008.

[144] J. Melen et al. Host Identity Protocol-based Mobile Router (HIPMR). IETF Draft, May 2009.

[145] L. Bokor, Z. Faigl, S. Imre, Survey and Evaluation of Advanced Mobility Management Schemes in the Host Identity Layer. International Journal of Wireless Networks and Broadband Technologies 3:(1) pp. 34-59. (2014), DOI: 10.4018/ijwnbt.2014010103.

[146] E. Rescorla. Diffie-Hellman Key AgreementMethod. RFC 2631 (Proposed Standard), June 1999.

[147] Z. Faigl, M. Telek, “Modeling the signaling overhead in Host-Identity Protocol-based secure mobile architectures,” Journal of Industrial Management and Optimization, vol. 11, no. 3, 2015, DOI: 10.3934/jimo.2015.11.887.

[148] Z. Faigl, “Performance Analysis of Signalling Overhead in Host Identity Protocol-based Secure Mobile Networks: Ultra Flat Architecture or End-to-End Signalling?,” Wireless Networks, 2014, DOI: 10.1007/s11276-014-0797-8.

[149] Werner Almesberger, Linux Network Traffic Control – Implementation Overview, EPFL ICA, April 23, 1999. URL: http://www.almesberger.net/cv/papers/tcio8.pdf

[150] Leonardo Balliache: Afhtb, URL: http://www.softwareopal.com/qos/default.php?p=ds-38 , checked in May 2014.

[151] V. Gurbani, M. Scharf, T. V. Lakshman, V. Hilt, and E. Marocco, "Abstracting network state in Software Defined Networks (SDN) for rendezvous services," in Proceedings of the IEEE International Conference on Communications (ICC), 2012, June 2012, pp. 6627–6632.

[152] V. Gurbani, V. Hilt, I. Rimac, M. Tomsu, and E. Marocco, "A survey of research on the application-layer traffic optimization problem and the need for layer cooperation," Communications Magazine, IEEE, vol. 47, no. 8, pp. 107–112, Aug. 2009.

[153] H. Xie, Y. R. Yang, A. Krishnamurthy, Y. G. Liu, and A. Silberschatz, "P4P: Provider Portal for Applications," in Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication (SIGCOMM '08), Seattle, WA, USA, Aug. 17-22, 2008, pp. 351–362.

[154] V. Aggarwal, A. Feldmann, and C. Scheideler, "Can ISPS and P2P Users Cooperate for Improved Performance?" SIGCOMM Comput. Commun. Rev., vol. 37, no. 3, pp. 29–40, Jul. 2007.

[155] D. Saucez, B. Donnet, and O. Bonaventure, "Implementation and Preliminary Evaluation of an ISP-driven Informed Path Selection," in Proceedings of the 2007 ACM CoNEXT Conference, ser. CoNEXT '07, 2007, pp. 45:1–45:2.

[156] D. Crockford, "The application/json Media Type for JavaScript Object Notation (JSON)," IETF RFC 4627, Jul. 2006.

[157] J. Medved, D. Ward, J. Peterson, R. Woundy, and D. McDysan, "ALTO Network-Server and Server-Server APIs," IETF Draft, draft-medvedalto-svr-apis-00, Mar. 2011.

[158] P. Racz and Z. Despotovic, "An ALTO Service based on BGP Routing Information," IETF Draft, draft-racz-bgp-based-alto-service-00, Jun. 2009.

[159] H. Gredler, J. Medved, S. Previdi, A. Farrel, and S. Ray, "North-Bound Distribution of Link-State and TE Information using BGP," IETF Draft, draft-ietf-idr-ls-distribution-04, Nov. 2013.

[160] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner,"OpenFlow: Enabling Innovation in Campus Networks," SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, April 2008.

[161] SDN definition on the ONF website: https://www.opennetworking.org/sdn-resources/sdn-definition

[162] ONF Solution Brief: OpenFlow™-Enabled Mobile and Wireless Networks, September 30, 2013. Wireless & Mobile Working Group, ONF,

[163] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner,"OpenFlow: Enabling Innovation in Campus Networks," SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, April 2008

[164] Sandvine: Global Internet Phenomena Report; 2011

[165] 3GPP: TS 23.203 Policy and Charging Control Architecture. 3GPP standard (2012);

[166] Ekström, H.: QoS Control in the 3GPP Evolved Packet System. In: IEEE Communications Magazine February 2009 pp. 76-83. IEEE Communications Society, New York (2009)

[167] Oyman, O., Singh, S.: Quality of Experience for HTTP Adaptive Streaming Services. In: IEEE Communications Magazine April 2012 pp. 20-27. IEEE Communications Society, New York (2012)

[168] Ouellette, S., Marchand, L., Pierre, S.: A Potential Evolution of the Policy and Charging Control/QoS Architecture for the 3GPP IETF-Based Evolved Packet Core. In: IEEE Communications Magazine May 2011 pp. 231-239. IEEE Communications Society, New York (2011)

[169] Alasti, M., Neekzad, B., Hui, L., Vannithamby, R.: Quality of Service in WiMAX and LTE Networks. In: IEEE Communications Magazine May 2010 pp. 104-111. IEEE Communications Society, New York (2010)

[170] Sterle, J., Volk, M., Sedlar, U., Bester, J., Kos, A.: Application-Based NGN QoE Controller. In: IEEE Communications Magazine January 2011 pp. 92-101. IEEE Communications Society, New York (2011)

[171] 3GPP: TS 29.212 Policy and Charging Control (PCC) over Gx/Sd reference point. 3GPP standard (2011);

[172] H. Kim and N. Feamster. "Improving network management with software defined networking." IEEE Commun. Mag., 51(2):114-119, February 2013.

[173] S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation Challenges for Software-Defined Networks," Communications Magazine, IEEE, vol. 51, no. 7, pp. 36–43, 2013.

[174] A. Lara, A. Kolasani, and B. Ramamurthy, "Network Innovation using OpenFlow: A Survey," Communications Surveys Tutorials, IEEE ,vol. PP, no. 99, pp. 1–20, 2013.

[175] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, "NOX: towards an operating system for networks," SIGCOMM Comput. Commun. Rev., vol. 38, no. 3, pp. 105–110, July 2008.

[176] Z. Cai, A. L. Cox, and T. S. E. Ng, "Maestro: A System for Scalable OpenFlow Control," Rice University, Tech. Rep., 2011.

[177] D. Erickson, "The beacon OpenFlow controller," in Proceedings of the second workshop on Hot topics in software defined networks, ser. HotSDN '13. New York, NY, USA: ACM, 2013.

[178] "Floodlight Is A Java-Based OpenFlow Controller," 2012. [Online]. Available: http://floodlight.openflowhub.org/

[179] T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, and S. Shenker, "Onix: a distributed control platform for large-scale production networks," in Proceedings of the 9th USENIX conference on Operating systems design and implementation, ser. OSDI'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–6.

[180] A. Tootoonchian and Y. Ganjali, "HyperFlow: a distributed control plane for OpenFlow," in Proceedings of the 2010 internet network management conference on Research on enterprise networking, ser. INM/WREN'10. Berkeley, CA, USA: USENIX Association, 2010.

[181] S. H. Yeganeh and Y. Ganjali. Kandoo: a framework for efficient and scalable offloading of control applications. In Proceedings of the first workshop on hot topics in software defined networks, HotSDN '12, pages 19–24, New York, NY, USA, 2012. ACM.

[182] M. Bansal, J. Mehlman, S. Katti, and P. Levis, "OpenRadio: A Programmable Wireless Dataplane," in Proceedings of the First Workshop on Hot Topics in Software Defined Networks, ser. HotSDN '12. New York, NY, USA: ACM, 2012, pp. 109-114.

[183] L. E. Li, Z. M. Mao, J. Rexford, "Toward Software-Defined Cellular Networks," Proc. EWSDN, Darmstadt, Germany, 2012.

[184] A. Gudipati, D. Perry, L. E. Li, and S. Katti. "Softran: software defined radio access network". In Proceedings of the second ACM SIGCOMM workshop on hot topics in software defined networking, pages 25–30. ACM SIGCOMM, 2013.

[185] S. B. H. Said, M. R. Sama, K. Guillouard, L. Suciu, G. Simon, X. Lagrange, and J.-M. Bonnin, "New control plane in 3GPP LTE/EPC architecture for on-demand connectivity service", in IEEE CLOUDNET, pp. 205-209, 2013.

[186] A. Basta, W. Kellerer, M. Hoffmann, K. Hoffmann, E.-D. Schmidt, "A Virtual SDN-Enabled LTE EPC Architecture: A Case Study for S-/P-Gateways Functions," IEEE SDN for Future Networks and Services (SDN4FNS), pp.1-7, Nov. 2013.

[187] A. Basta, W. Kellerer, M. Hoffmann, H. Morper, K. Hoffmann, "Applying NFV and SDN to LTE Mobile Core Gateways; The Functions Placement Problem", AllThingsCellular14, Workshop ACM SICGOMM (accpeted for publication), Chicago, IL, USA, August 2014.

[188] R. Haw, S.C. Hong, S. Lee, "An efficient content delivery framework for SDN based LTE network", IMCOM (ICUIMC)'14, January 9-11, 2014, Siem Reap, Cambodia.

[189] J. Costa-Requena, "SDN integration in LTE mobile backhaul networks," Information Networking (ICOIN), 2014 International Conference on, vol., no., pp.264--269, 10-12 Feb. 2014.

[190] J. Kempf, B. Johansson, S. Pettersson, H. Luning, T. Nilsson, "Moving the Mobile Evolved Packet Core to the Cloud," Proc. WiMob, Barcelona, Spain, 2012.

[191] K. Pentikousis, Y. Wang, and W. Hu, "MobileFlow: Toward Software- Defined Mobile Networks," IEEE Communications Magazine, vol. 51, pp. 44–53, July 2013.

[192] H. Ali-Ahmad, C. Cicconetti, A. de la Oliva, M. Draxler, R. Gupta, V. Mancuso, L. Roullet, and V. Sciancalepore, "CROWD: An SDN approach for densenets," in Software Defined Networks (EWSDN), 2013 Second European Workshop on, Oct 2013, pp. 25-31.

[193] S. Auroux, M. Draxler, A. Morelli, V. Mancuso "CROWD Dynamic Network Reconfiguration in Wireless DenseNets" European Conference on Networks and Communications (EuCNC'14) - Sébastien

[194] M. Yang, Y. Li, D. Jin, L. Su, S. Ma, and L. Zeng, "OpenRAN: a software-defined ran architecture via virtualization," in Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, ser. SIGCOMM '13. New York, NY, USA: ACM, 2013, pp. 549-550.

[195] G. Savarese, M. Vaser, M. Ruggieri, "A Software Defined Networking-based context-aware framework combining 4G cellular networks with M2M," Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on, vol., no., pp.1-6, 24-27 June 2013

[196] J. G. Andrews, S. Buzzi, W. Choi, S. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5G be?" IEEE Journal on Selected Areas in Communications, Sep. 2014.

[197] R. Li, Z. Zhao, X. Zhou, J. Palicot, H. Zhang, "The prediction analysis of cellular radio access network traffic: From entropy theory to networking practice," Communications Magazine, IEEE , vol.52, no.6, pp.234,240, June 2014

[198] Ericsson, "The Real-Time Cloud," White Paper, Uen 284 23-3219 Rev B, February 2014.

[199] V. Yazici, U. Kozat, M.O. Sunay, "A New Control Plane for 5G Network Architecture with a Case Study on Unified Handoff, Mobility, and Routing Management," IEEE Communications Magazine, November 2014.

[200] R. Raghavendra, J. Lobo, K-W. Lee, "Dynamic Graph Query Primitives for SDN-Based Cloud Network Management, Proceedings of ACM HotSDN, 2012.

[201] P. Sun, M. Yu, M.J. Freedman, J. Rexford, D. Walker, "HONE: Joint Host-Network Traffic Management in Software-Defined Networks," to appear in the Journal of Network and Systems Management, 2014.

[202] R. Cannistra, B. Carle, M. Johnson, J. Kapaida, Z. Meath, M. Miller, D. Young, C. DeCusatis, T. Bundy, G. Zussman, K. Bergman, A. Carranze, C. Sher-DeCusatis, A. Pletch, R. Ransom, "Enabling Autonomic

Provisioning in SDN Cloud Networks with NFV Service Chaining," Proceedings of Optical Fiber Communications Conference and Exhibition, 2014.

[203] W-C. Lin, C-H. Liao, K-T. Kuo, C. H.-P. Wen, "Flow-and-VM Migration for Optimizing Throughput and Energy in SDN-Based Cloud Datacenter," Proceedings of CloudCom, 2013.

[204] C. DeCusatis, M. Haley, T. Bundy, "Dynamic, Software-Defined Service Provider Infrastructure and Cloud Drivers fort SDN Adoption," Proceedings of the IEEE ICC, 2013.

[205] W. Hong, K. Wang, and Y.-H. Hsu, "Application-Aware Resource Allocation for SDN-based Cloud Datacenters," in 2013 International Conference on Cloud Computing and Big Data, 2013, pp. 106–110.

[206] B. Martini, D. Adami, A. Sgambelluri, M. Gharbaoui, L. Donatini, S. Giordano, and P. Castoldi, "An SDN orchestrator for resources chaining in cloud data centers," in 2014 European Conference on Networks and Communications (EuCNC), 2014, pp. 1–5.

[207] J. Pettit, "Open vSwitch and the Intelligent Edge," OpenStack Summit, Atlanta, May 13, 2014.

A. Appendix - Foundations of Network Resource Management: Protocols

A.1 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

A.1.1 Overview

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an *agent* which reports information via SNMP to the manager.

Essentially, SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

An SNMP-managed network consists of three key components:

- Managed device
- Agent — software which runs on managed devices
- Network management system (NMS) — software which runs on the manager

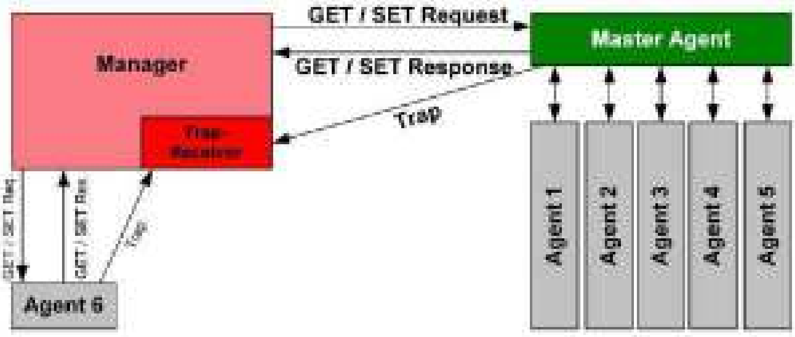


Figure 1 – Principle of SNMP communication.

A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A *network management system* (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

A.1.2 Management Information Base (MIB)

SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP. MIBs use the notation defined by Structure of Management Information Version 2 (SMIv2, RFC 2578), a subset of ASN.1.

A.1.3 Protocol Details

SNMP operates in the Application Layer of the Internet Protocol Suite. The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (Traps and InformRequests) on port 162. The agent may generate notifications from any available port. When used with Transport Layer Security or Datagram Transport Layer Security requests are received on port 10161 and traps are sent to port 10162.

SNMPv1 specifies five core protocol data units (PDUs). Two other PDUs, *GetBulkRequest* and *InformRequest* were added in SNMPv2 and carried over to SNMPv3.

All SNMP PDUs are constructed as follows:

IP header	**UDP header**	**version**	**community**	**PDU-type**	**request-id**	**error-status**	**error-index**	**variable bindings**

The seven SNMP protocol data units (PDUs) are as follows:

- **GetRequest**

  A **manager-to-agent** request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A *Response* with current values is returned.

- **SetRequest**

  A **manager-to-agent** request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A *Response* with (current) new values for the variables is returned.

- **GetNextRequest**

  A **manager-to-agent** request to discover available variables and their values. Returns a *Response* with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of *GetNextRequest* starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

- **GetBulkRequest**

  Optimized version of *GetNextRequest*. A **manager-to-agent** request for multiple iterations of *GetNextRequest*. Returns a *Response* with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific *non-repeaters* and *max-repetitions* fields are used to control response behavior. *GetBulkRequest* was introduced in SNMPv2.

- **Response**

  Returns variable bindings and acknowledgement from **agent to manager** for *GetRequest*, *SetRequest*, *GetNextRequest*, *GetBulkRequest* and *InformRequest*. Error reporting is provided by *error-status* and *error-index* fields. Although it was used as a response to both gets and sets, this PDU was called *GetResponse* in SNMPv1.

- **Trap**

  Asynchronous notification from **agent to manager**. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. Includes current *sysUpTime* value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed *SNMPv2-Trap*.

- **InformRequest**

  Acknowledged asynchronous notification. This PDU was introduced in SNMPv2 and was originally defined as **manager to manager** communication. Later implementations have loosened the original definition to allow **agent to manager** communications. Manager-to-manager notifications were already possible in SNMPv1 (using a *Trap*), but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a *Trap* was not guaranteed. *InformRequest* fixes this by sending back an acknowledgement on receipt.

A.1.4 Development and Usage : SNMP versions

A.1.4.1 Version 1

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used and is the de facto network-management protocol in the Internet community.

The first RFCs for SNMP, now known as SNMPv1, appeared in 1988:

- **RFC 1065**: Structure and identification of management information for TCP/IP-based internets
- **RFC 1066**:Management information base for network management of TCP/IP-based internets
- **RFC 1067**: A simple network management protocol

These protocols were obsoleted by:

- **RFC 1155**: Structure and identification of management information for TCP/IP-based internets
- **RFC 1156**: Management information base for network management of TCP/IP-based internets
- **RFC 1157**: A simple network management protocol

After a short time, RFC 1156 (MIB-1) was replaced by more often used:

- **RFC 1213**: Version 2 of management information base (MIB-2) for network management of TCP/IP-based internets

Version 1 has been criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext. The '80s design of SNMP V1 was done by a group of collaborators who viewed the officially sponsored OSI/IETF/NSF (National Science Foundation) effort (HEMS/CMIS/CMIP) as both unimplementable in the computing platforms of the time as well as potentially unworkable. SNMP was approved based on a belief that it was an interim protocol needed for taking steps towards large scale deployment of the Internet and its commercialization. In that time period Internet-standard authentication/security was both a dream and discouraged by focused protocol design groups.

A.1.4.2 Version 2

SNMPv2 (RFC 1441–RFC 1452), revises version 1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced *GetBulkRequest*, an alternative to iterative GetNextRequests for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMPv2, viewed by many as overly complex, was not widely accepted.

Community-Based Simple Network Management Protocol version 2, or *SNMPv2c,* is defined in RFC 1901–RFC 1908. In its initial stages, this was also informally known as *SNMPv1.5*. SNMPv2c comprises SNMPv2 *without* the controversial new SNMP v2 security model, using instead the simple community-based security scheme of SNMPv1. While officially only a "Draft Standard", this is widely considered the *de facto* SNMPv2 standard.

User-Based Simple Network Management Protocol version 2, or *SNMPv2u,* is defined in RFC 1909–RFC 1910. This is a compromise that attempts to offer greater security than SNMPv1, but without incurring the high complexity of SNMPv2. A variant of this was commercialized as *SNMP v2**, and the mechanism was eventually adopted as one of two security frameworks in SNMP v3.

A.1.4.3 Version 3

Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, it looks much different due to new textual conventions, concepts, and terminology.

SNMPv3 primarily added security and remote configuration enhancements to SNMP. Due to lack of security with the use of SNMP, network administrators were using other means, such as telnet for configuration, accounting, and fault management. SNMPv3 addresses issues related to the large-scale deployment of SNMP, accounting, and fault management. Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities. SNMPv3 provides a secure environment for the management of systems covering the following. Identification of SNMP entities to facilitate communication only between known SNMP entities - Each SNMP entity has an identifier called the SNMPEngineID, and SNMP communication is possible only if an SNMP entity knows the identity of its peer. Traps and Notifications are exceptions to this rule. Support for security models - A security model may define the security policy within an administrative domain or an intranet. SNMPv3 contains the specifications for USM. Definition of security goals where the goals of message authentication service include protection against the following. Modification of Information - Protection against some unauthorized SNMP entity altering in-transit messages generated by an authorized principal. Masquerade - Protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations. Message Stream Modification - Protection against messages getting maliciously re-ordered, delayed, or replayed to effect unauthorized management operations. Disclosure - Protection against eavesdropping on the exchanges between SNMP engines. Specification for USM - USM consists of the general definition of the following communication mechanisms available. Communication without authentication and privacy (NoAuthNoPriv). Communication with authentication and without privacy (AuthNoPriv). Communication with authentication and privacy (AuthPriv). Definition of different authentication and privacy protocols - Currently, the MD5 and SHA authentication protocols and the CBC_DES and CFB_AES_128 privacy protocols are supported in the USM. Definition of a discovery procedure - To find the SNMPEngineID of an SNMP entity for a given transport address and transport endpoint address. Definition of the time synchronization procedure - To facilitate authenticated communication between the SNMP entities. Definition of the SNMP framework MIB - To facilitate remote configuration and administration of the SNMP entity. Definition of the USM MIBs - To facilitate remote configuration and administration of the security module. Definition of the VACM MIBs - To facilitate remote configuration and administration of the access control module. The SNMPv3 focuses on two main aspects, namely security and administration. The security aspect is addressed by offering both strong authentication and data encryption for privacy. The administration aspect is focused on two parts, namely notification originators and proxy forwarders.

SNMPv3 defines two security-related capabilities, namely the USM and VACM. USM provides authentication and privacy (encryption) functions and operates at the message level. VACM determines whether a given principal is allowed access to a particular MIB object to perform specific functions and operates at the PDU level. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent. Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

- **Confidentiality**: Encryption of packets to prevent snooping by an unauthorized source.
- **Integrity:** Message integrity to ensure that a packet has not been tampered while in transit including an optional packet replay protection mechanism.
- **Authentication:** To verify that the message is from a valid source.

As of 2004 the IETF recognizes *Simple Network Management Protocol version 3* as defined by RFC 3411–RFC 3418 (also known as STD0062) as the current standard version of SNMP. The IETF has designated SNMPv3 a full Internet standard, the highest maturity level for an RFC. It considers earlier versions to be obsolete (designating them "Historic").

In practice, SNMP implementations often support multiple versions: typically SNMPv1, SNMPv2c, and SNMPv3.

A.1.5 Security Implications

SNMP versions 1 and 2c are subject to *packet sniffing* of the clear text community string from the network traffic, because they do not implement encryption.

Another security issue is that all versions of SNMP are subject to *brute force* and *dictionary attacks* for guessing the community strings, authentication strings, authentication keys, encryption strings, or encryption keys, because they do not implement a *challenge-response handshake*. It is important to emphasize that although SNMP works over TCP and other protocols, it is most commonly used over UDP that is connectionless and vulnerable to IP spoofing attacks. Thus, all versions are subject to bypassing device access lists that might have been implemented to restrict SNMP access, though SNMPv3's other security mechanisms should prevent a successful attack. SNMP's powerful configuration (write) capabilities are not being fully utilized by many vendors, partly because of a lack of security in SNMP versions before SNMPv3 and partly because many devices simply are not capable of being configured via individual MIB object changes.

A.2 Network Configuration Protocol (NETCONF)

The NETCONF protocol defines a simple mechanism through which a network device can be managed, configuration data information can be retrieved, and new configuration data can be uploaded and manipulated. The protocol allows the device to expose a full, formal application programming interface (API). Applications can use this straightforward API to send and receive full and partial configuration data sets.

The NETCONF protocol uses a remote procedure call (RPC) paradigm. A client encodes an RPC in XML [1] and sends it to a server using a secure, connection-oriented session. The server responds with a reply encoded in XML.The contents of both the request and the response are fully described in XML DTDs or XML schemas, or both, allowing both parties to recognize the syntax constraints imposed on the exchange.

A key aspect of NETCONF is that it allows the functionality of the management protocol to closely mirror the native functionality of the device. This reduces implementation costs and allows timely access to new features. In addition, applications can access both the syntactic and semantic content of the device's native user interface.

NETCONF allows a client to discover the set of protocol extensions supported by a server. These "capabilities" permit the client to adjust its behaviour to take advantage of the features exposed by the device. The capability definitions can be easily extended in a non-centralized manner. Standard and non-standard capabilities can be defined with semantic and syntactic rigor.

The NETCONF protocol is a building block in a system of automated configuration. XML is the lingua franca of interchange, providing a flexible but fully specified encoding mechanism for hierarchical content. NETCONF can be used in concert with XML-based transformation technologies, such as XSLT (Extensible Stylesheet Language Transformations), to provide a system for automated generation of full and partial configurations. The system can query one or more databases for data about networking topologies, links, policies, customers, and services. This data can be transformed using one or more XSLT scripts from a task-oriented, vendor-independent data schema into a form that is specific to the vendor, product, operating system, and software release. The resulting data can be passed to the device using the NETCONF protocol.

A.2.1 Overview

NETCONF uses a simple RPC-based mechanism to facilitate communication between a client and a server. The client can be a script or application typically running as part of a network manager. The server is typically a network device. The terms "device" and "server" are used interchangeably in this document, as are "client" and “application".

A NETCONF session is the logical connection between a network administrator or network configuration application and a network device. A device must support at least one NETCONF session and should support multiple sessions. Global configuration attributes can be changed during any authorized session, and the effects are visible in all sessions. Session-specific attributes affect only the session in which they are changed.

NETCONF can be conceptually partitioned into four layers:

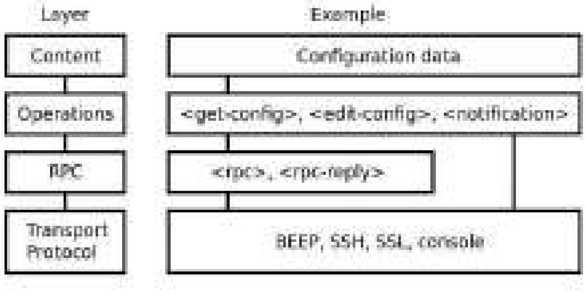


Figure 2 – NETCONF protocol layers.

1. The transport protocol layer provides a communication path between the client and server. NETCONF can be layered over any transport protocol that provides a set of basic requirements. Section 2 discusses these requirements.
2. The RPC layer provides a simple, transport-independent framing mechanism for encoding RPCs. Section 4 documents this protocol.
3. The operations layer defines a set of base operations invoked as RPC methods with XML-encoded parameters. Section 7 details the list of base operations.

4. The content layer is outside the scope of this document. Given the current proprietary nature of the configuration data being manipulated, the specification of this content depends on the NETCONF implementation. It is expected that a separate effort to specify a standard data definition language and standard content will be undertaken.

A.2.2 Capabilities

A NETCONF capability is a set of functionality that supplements the base NETCONF specification. The capability is identified by a uniform resource identifier (URI). Capabilities augment the base operations of the device, describing both additional operations and the content allowed inside operations.

The client can discover the server's capabilities and use any additional operations, parameters, and content defined by those capabilities.

The capability definition may name one or more dependent capabilities. To support a capability, the server MUST support any capabilities upon which it depends.

A.2.3 Separation of Configuration and State Data

The information that can be retrieved from a running system is separated into two classes, configuration data and state data. Configuration data is the set of writable data that is required to transform a system from its initial default state into its current state. State data is the additional data on a system that is not configuration data such as read-only status information and collected statistics. When a device is performing configuration operations, a number of problems would arise if state data were included:

- Comparisons of configuration data sets would be dominated by irrelevant entries such as different statistics.
- Incoming data could contain nonsensical requests, such as attempts to write read-only data.
- The data sets would be large.
- Archived data could contain values for read-only data items, complicating the processing required to restore archived data.

To account for these issues, the NETCONF protocol recognizes the difference between configuration data and state data and provides operations for each. The <get-config> operation retrieves configuration data only, while the <get> operation retrieves configuration and state data.

Note that the NETCONF protocol is focused on the information required to get the device into its desired running state. The inclusion of other important, persistent data is implementation specific. For example, user files and databases are not treated as configuration data by the NETCONF protocol.

If a local database of user authentication data is stored on the device, whether it is included in configuration data is an implementation-dependent matter.

A.3 Internet Control Message Protocol (ICMP)

ICMP is considered one of the core protocols in the Internet Protocol (IP) suite. Unlike the common data transfer protocols, such as TCP and UDP, ICMP is not typically used by applications as a method of communication. Rooted in the IP portion of TCP/IP, ICMP operates outside the rules of traditional TCP and UDP.

This isolation from the common data transfer protocols is what gives ICMP great power in troubleshooting and otherwise managing your network. Its protocol specification enjoys an extremely limited set of commands, which are restricted by design to the tasks of exploring host and network connectivity and routing. As such, ICMP traffic is commonly available in all but the most highly-secured of networks.

A.4 TL1 (Transaction Language 1)

Transaction Language 1 (TL1) is a widely used management protocol in telecommunications. It is a cross-vendor, cross-technology man-machine language, and is widely used to manage optical (SONET) and broadband access infrastructure in North America. TL1 is used in the input and output messages that pass between Operations Systems (OSs) and Network Elements (NEs). Operations domains such as surveillance, memory administration, and access and testing define and use TL1 messages to accomplish specific functions between the OS and the NE. TL1 is defined in Telcordia Technologies (formerly Bellcore) Generic Requirements document GR-831-CORE. TL1 is a set of ASCII-based instructions, or "messages". These messages enable a human user or an Operations Support System (OSS) to manage a network element (NE) and its resources.

In addition to being open, TL1 is powerful because it bridges the gap between human users and network equipment. It is structured enough to be parsed by machines, but also verbose enough to be read by human operators. Since special decoders or debuggers are not necessary, TL1 is a frequent command line interface choice for equipment manufacturers. TL1 messages are also embedded with the database information required to interpret the meaning of an alarm.

B. Appendix – QoS provisioning in 3GPP EPC

Connectivity to Packet Data Networks is provided by PDN connections in 2G/3G packet core and in EPC. A PDN connection comprises several aspects, i.e., IP access, in-band QoS provisioning, mobility and charging.

PDN connections are provided by PDP contexts in the 2G/3G core (between the UE and GGSN), and EPS bearers in EPC for E-UTRAN access (between the UE and P-GW). Several options are available to provide PDN connection between 2G/3G access and P-GW or E-UTRAN and GGSN. E-g., an UE can access from a 2G/3G RAN the SGSN through PDP context, have a one-to-one mapping between PDP contexts and EPS bearers in the SGSN, and reach the S-GW and P-GW with EPS bearers.

2G/3G supports two types of PDP contexts related to IP connectivity: IPv4 and IPv6. A PDN connection in EPC supports IPv4, IPv6 and both IPv4 and IPv6 address allocation to the UE within the same PDN connection. It can be noted that in 3GPP Release 9, support for dual stack PDP context is also introduced in the 2G/3G GPRS core network. IP address is allocated during the Attach (PDP context activation) procedure to the UE. Another option is the usage of DHCPv4 after attach procedure or PDP context activation. DHCPv6 is not supported. Stateless IPv6 address autoconfiguration is also supported by sending routing advertisements through the PDN connection advertising a /64 bit prefix allocated to the specific PDN connection.

For E-UTRAN access in EPS, EPS bearer is a basic tool to handle QoS. In fact, the PDN connectivity is provided by one default bearer, and optionally other dedicated bearers. Each EPS bearer is associated with a set of QoS parameters, and a traffic flow template (TFT) which specifies the traffic filters related to which IP flows must be mapped to the specific EPS bearer. TFTs may contain traffic filters for downlink and uplink traffic (denoted by DL TFT, UL TFT, respectively).

The filter information is typically the 5-tuple of source and destination IP addresses, transport protocol, source and destination ports. Wildcards can be used to define a range of addresses or ports. Other parameters of traffic filters can be the IPsec Security Parameter Index, Type of Service (IPv4)/Traffic Class (IPv6) or Flow Label (IPv6).

All traffic flows matching the traffic filters of an EPS bearer will get the same QoS treatment. Multiple EPS bearers can belong to the same PDN connection.

During the Attach procedure, a default bearer is established to provide always-on connectivity for the UE. In 2G/3G GPRS core, this looks differently, because PDP contexts are only activated when an application requests IP connection.

EPS has adopted network-centric QoS control approach, i.e., it is basically only the P-GW, which can activate, de-activate, modify EPS bearers and decide flow mapping to EPS bearers. That is different in pre-EPS systems. Originally, in 2G/3G GPRS it was only the UE that could initiate new PDP context activation and decide about flow mapping to PDP contexts. Then, in 3GPP Release 7, network-requested secondary PDP context activation has been introduced, where the GGSN initiates the creation of a new “bearer” (PDP context) and assigns IP flows to the bearer. This change is due to the introduction of policy control within the 2G/3G GPRS core and in EPC.

The GPRS Tunneling Protocol (GTP) is responsible for the control of PDP contexts in 2G/3G GGSN core (GTP-C) and the tunneling of IP packets of the user (GTP-U).

For EPC a new version for the GTP-C has been developed to manage EPS bearers over the S1, S5/S8 interfaces, but the tunneling of user IP traffic remains the same as it was. This is called GTPv2.

Depending on the tunneling option, EPS bearers are implemented in different ways.

Figure 58 represents the hierarchy and terminology of bearers for E-UTRAN access.

For E-E QoS provision, an EPS bearer and an External bearer (not managed by the MNO) are required. An EPS bearer consists of an E-RAB and an S5/S8 bearer. An E-RAB includes a Radio Bearer and an S1 bearer.

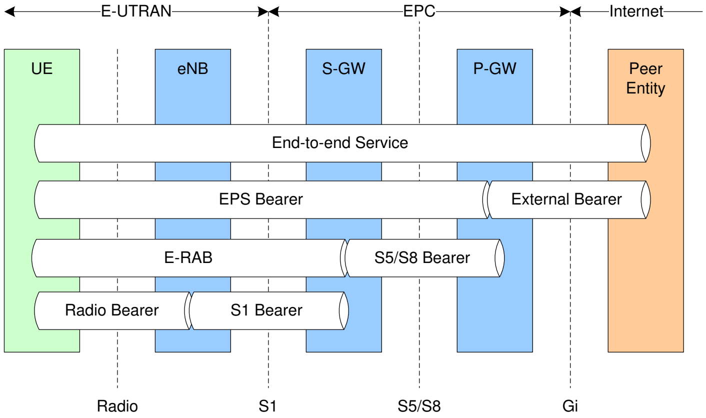


Figure 58 - Hierarchy of bearers.

Figure 59 presents the realization of EPS bearers in the user plane when E-UTRAN access and GTP-based S5/S8 is used

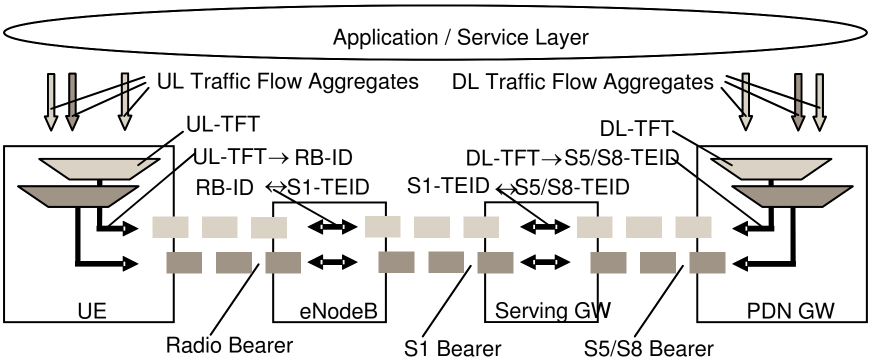


Figure 59 - EPS bearer in E-UTRAN access and GTP-based S5/S8 [4].

Figure 60 illustrates the realization of EPS bearers in the user plane when PMIP/IP GRE-based S5/S8 interface is applied.

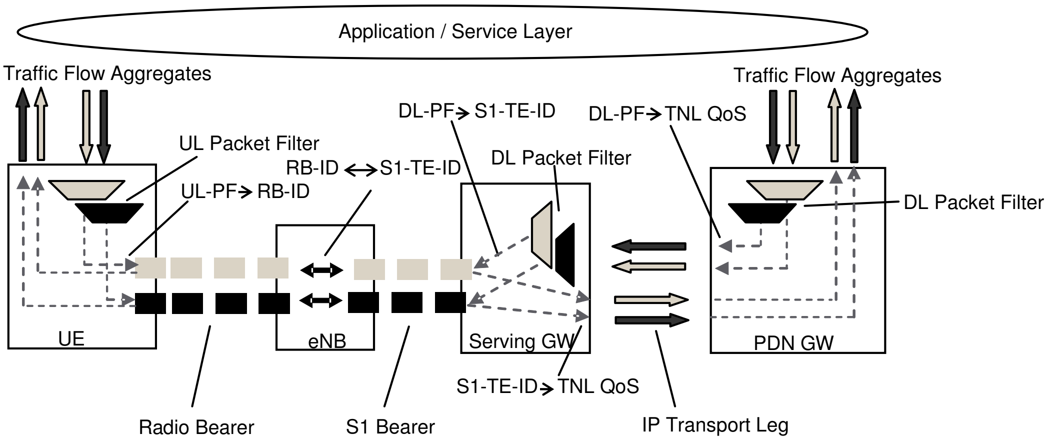


Figure 60 - EPS bearer in E-UTRAN access and PMIP/IP GRE-based S5/S8 [5].

Figure 61 illustrates the case of untrusted non-3GPP access when GTP tunneling is used between the P-GW and ePDG.

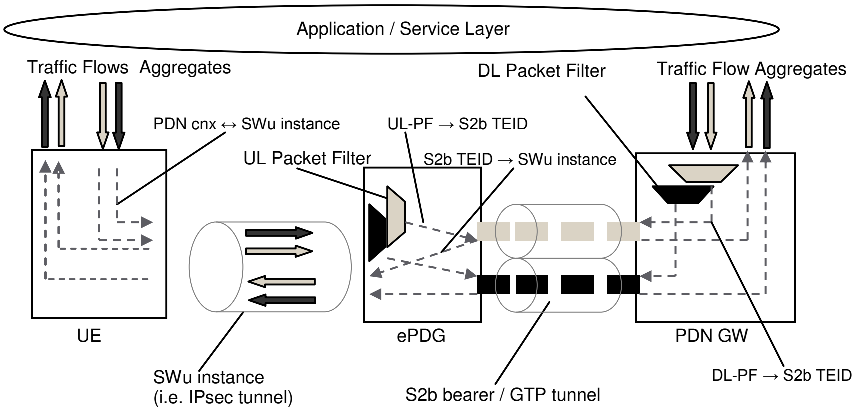


Figure 61 – EPS bearer in case of untrusted non-3GPP access and GTP-based S2b interface [5].

When the EPS bearer is realized with GTP-U tunnels on the S1 interface and optionally on the S5/S8, S2a, S2b interface the QoS is controlled using on-path solution, i.e., EPS bearer establishment, modification, deletion procedures of GTPv2-C.

In Figure 59, the EPS bearer is realized with the concatenation of Radio Bearer, a GTP-U S1 bearer and a GTP-U S5/S8 bearer.

Figure 60 illustrates that the EPS bearer consists of the concatenation of the Radio bearer and a GTP-U S1 bearer when PMIP/IP GRE tunneling is used on the S5/S8 interface.

Figure 61 illustrates the case of untrusted non-3GPP IP access over S2b interface. If GTPv2 is used on the S2b interface, then on-path EPS bearer management is supported towards the ePDG. However, since the access network is not managed by the provider, the MNO cannot provide guaranteed QoS services on the Swu interface between the UE and the ePDG. The UE must establish separate SWu instance (i.e. a separate IPSec tunnel) for each PDN connection, when GTP is used on S2b, enabling one-to-one mapping of EPS bearers and IPsec tunnels.

PMIP does not support any QoS bearer concept. When PMIP/IP GRE is applied on an Sx interface then the transport network layer is responsible to provide appropriate QoS guarantees for the service data flows.

Bearer binding means that the appropriate bearer is allocated for service data flows in order to provide appropriate QoS treatment. When PMIP tunneling is used then bearer binding is not made on the P-GW but on the network element where the bearers are ending. Hence,

- in case of PMIP tunneling on S5/S8, the S-GW is responsible for bearer binding,
- in case of trusted non-3GPP access, the gateway, which implements QoS bearers for the non-3GPP access (e.g., High Rate Packet Data Serving GW in cdma2000 access), may provide bearer binding function.

Due to the fact that there is no on-path bearer control between the P-GW and the bearer binding function in case of PMIP-based tunneling, there is a need for off-path policy control mechanism. The Policy Control and Charging function of EPC generalizes the concept of EPS bearers, and provides an off-path bearer control framework for any access network that includes bearer binding function in its GW.

Packet filters enable the binding of flows to the appropriate EPS bearer. For E-UTRAN access, UL TFTs are deployed the UE (as shown by Figure 59 and Figure 60). In untrusted non-3GPP access UL TFTs are deployed in the ePDG (presented in Figure 61). DL TFTs are deployed always by the Policy Control Enforcement Function (PCEF) in the P-GW.

If bearer binding function is separated from PCEF, e.g., in case of PMIP-based S5/S8 (illustrated in Figure 60) or S2a, then DL TFTs are also deployed in the GW, which is responsible for the bearer binding function. P-GW does not need bearer mapping for DL traffic in that case, but still performs bit rate enforcement (for the aggregate of non-guaranteed bitrate traffic in UL and DL) and charging for the different IP flows. The GW which enforces bearer binding can enforce bitrate for GBR traffic in DL.

B.1 QoS for EPS bearers

EPS differentiates two types of EPS bearers:

- Guaranteed Bit-Rate (GBR) bearers are typically used for those services where it is better to block a service rather than degrade already admitted services. E.g., VoIP, video streaming benefit from a constant bandwidth, hence GBR is needed to provide satisfactory user experience. An important characteristic of GBR bearer is that it is associated with a certain amount of bandwidth, independently of being utilized or not. The GBR always takes up resources over the radio link, even If no traffic is sent. Hence, in normal cases the GBR bearer should not experience any packet loss.
- Non-GBR bearers are used for those services which normally do not require a constant fixed bandwidth, such as web browsing, e-mail, chat etc. No transmission resource are reserved for non-GBR bearers.

Dropping a GBR EPS bearer in case of congestion in the network is required in the following situation. The E UTRAN/UTRAN and the UE support the RFC 3168 Explicit Congestion Notification (ECN) [6]. The IP level ECN scheme enables the E UTRAN/UTRAN to trigger a rate adaptation scheme at the application / service / transport layer. To make sufficient time available for end-to-end codec rate adaptation the E-UTRAN/UTRAN should attempt to not drop any packets on a bearer for a default grace period of at least 500 ms after it has indicated congestion with ECN on the bearer for packets within the packet delay budget. During this ECN grace period the E-UTRAN/UTRAN should also attempt to meet the QCI characteristics / QoS class associated with the bearer. The EPC does not support E-UTRAN/UTRAN-initiated "QoS re-negotiation". That is, the EPC does not support an eNodeB/RNC initiated bearer modification procedure. If an eNodeB/RNC can no longer sustain the GBR of an active GBR bearer then the eNodeB/RNC should simply trigger a deactivation of that bearer.

An EPS bearer QoS profile however is broader than this categorization. It includes the parameters QCI, ARP, GBR and MBR, defined in the following.

For both non-GBR and GBR services QoS parameters are the following:

- QoS Class Identifier (QCI): QCI is just a pointer to node specific parameters, which define what packet forwarding treatment a particular bearer should receive (scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration etc.). On radio interfaces and S1 interface each protocol data unit is indirectly associated with one QCI via the bearer identifier carried in the header. Same applies to S5, S8 if GTP based option is used. In GTP-U the identifier is the Tunnel Endpoint Identifier (TEID) conveyed in the GTP header. Appendix B.5 summarizes the characteristics of standardized QCI values. Standardized QCI values guarantee that applications receive the same QoS treatment in multi-vendor environments.
- Allocation and Retention Priority (ARP): ARP is used indicate the priority for the allocation and retention of bearers. It includes
    - priority level: higher priority establishment and modification requests are preferred in situations where resources are scarce
    - pre-emption capability: if true, then this bearer request could drop away another lower priority bearer
    - pre-emption vulnerability: if true than this bearer can be dropped by a higher priority bearer establishment/modification

QoS parameters for GBR bearer:

- Guaranteed Bit Rate (GBR): is the minimum bitrate that an EPS bearer should get
- Maximum Bit Rate (MBR). The MBR limits the bit rate that can be expected to be provided by a GBR bearer (e.g. excess traffic may get discarded by a rate shaping function). Currently MBR is set to the same value as GBR in EPC, i.e., the instantaneous rate can never be greater than the GBR for GBR bearers.

Aggregate QoS parameters for non-guaranteed bearers (aggregate values):

- Per APN Aggregate Maximum Bit Rate (APN-AMBR): It defines the total bitrate that is allowed to be used by the user for all non-GBR bearers associated with a specific APN. It is enforced by P-GW in DL and the UE and P-GW in UL.
- Per UE Aggregate Maximum Bit Rate (UE-AMBR): The UE-AMBR limits the aggregate bitrate of all non-GBR bearers of the user. It is enforced by the eNodeB in UL and DL. The actually

enforced rate is the minimum of the sum of all active APN's APN-AMBR and the subscribed UE-AMBR value.

The HSS defines, for each PDN subscription context, the 'EPS subscribed QoS profile' which contains

- the bearer level QoS parameter values for the default bearer (QCI and ARP) and
- the subscribed APN-AMBR value.

The subscribed ARP shall be used to set the priority level of the EPS bearer parameter ARP for the default bearer. In addition, the subscribed ARP shall be applied by the P-GW for setting the ARP priority level of all dedicated EPS bearers of the same PDN connection unless a specific ARP priority level setting is required (due to P-GW configuration or interaction with the PCRF). The pre-emption capability and the pre-emption vulnerability information for the default bearer are set based on MME operator policy.

The mapping of services to GBR and non-GBR bearers is the choice of the operator, and can be controlled with static rules in the PCEF, or dynamic PCC and QoS rules by the PCC framework.

B.2 QoS for non-3GPP access

In GERAN/UTRAN accesses a more complicated QoS concept is used, hence operators are not using many of the parameters in practice. That concept is referred to as the release 99 QoS. Its main characteristics are the following:

- 4 Traffic classes, one mapped at the same time to a PDP context
- 13 attributes, e.g., bitrate, priority, error rate, max. delay etc

For GERAN/UTRAN access to EPS via S4 based SGSN the QoS attributes must be translated from release 99 QoS to EPS QoS parameters, when one-to-one mapping of PDP contexts to EPS bearers is performed. Mapping is described in Annex E of TS 23.401 [4].

B.3 QoS enforcement in EPS

The following QoS treatment functions are deployed in the user plane of E-UTRAN and EPC. The maximum granularity of QoS control achieved by these functions is the EPS bearer granularity.

- PCEF enforces traffic gating control for UL and DL based on policies
- mapping packets to actual EPS bearer using TFTs:
    - UE for UL
    - P-GW for DL, if GTP-based S5/S8
    - S-GW for DL, if PMIP-based S5/S8
- admission control (bearer establishment, modification) and preemption handling (congestion control, bearer drop) when resources are scarce, using the ARP to differentiate the handling of bearers:
    - eNodeB
    - P-GW, if GTP-based S5/S8
    - S-GW if PMIP-based S5/S8
- rate policing
    - eNodeB enforces the maximum rate for the aggregate of non-GBR bearers of the UE in UL and DL, based on the UE-AMBR UL and DL values.
    - P-GW enforces the maximum rate for the aggregate of non-GBR bearers of the UE in UL and DL, using APN-AMBR values for UL and DL
    - eNodeB enforces GBR/MBR for GBR-bearers in UL
    - P-GW enforces GBR/MBR for GBR bearers in DL, if GTP-based S5/S8
    - S-GW enforces GBR/MBR for GBR bearers in DL, if PMIP-based S5/S8
- queue management, scheduling and configuration of L1/L2 protocols to enforce QCI characteristics, such as packet delay budget and packet loss in E-UTRAN
    - eNodeB in UL and DL
- map QCI to DSCP for IP transport network between EPC elements, e.g.:
    - eNB, S-GW, for IP transport between eNodeB and S-GW
    - S-GW, P-GW, for IP transport between S-GW and P-GW
- enforce QoS on the path of EPS bearers in the transport network layer
    - routers, switches deploy queue management, UL/DL scheduling

B.4 Policy and charging control in 3GPP

Policy and charging control (PCC) provides QoS and charging control for operators. It provides a general, centralized framework to control the QoS procedures of heterogeneous access networks. It supports control of the user plane for IP Multimedia Subsystem (IMS) and non-IMS services. It solves the problem of lacking on-path QoS control in case of non-GTP based tunneling options by off-path control using the Diameter protocol, if the access network provides QoS bearers.

The 'bearer' in PCC denotes an IP data path with desired QoS characteristics, hence is more generic than EPS bearer/ PDP context and access agnostic. Multiple service sessions can be transported over the same bearer. PCC enables service-aware QoS control, having higher granularity than the bearer-level QoS control provided by EPS bearers. PCC allows QoS control over wireless non-3GPP access networks, such as HRPD and WiMAX. For the fixed access, interworking with policy control has not come as far as for the wireless access. It supports policy control in roaming scenarios as well.

B.4.1 Diameter QoS application for the support of IntServ and DiffServ

Two concepts for applying QoS are the Integrated and Differentiated Services. IntServ work on per flow/service level and is based on RSVP signaling protocol. Basically the source sends RSVP path message and requests from each network node up to the receiver to reserve certain capacity. The nodes reply with an RSVP RESV message that contains a confirmation of the reserved bandwidth. Due to the huge signaling overhead the Intserv approach is not widely used today. The only place where it is still popular is MPLS traffic engineering clouds. Therefore the extension of RSVR - RSVP TE is used for reserving huge capacities in providers' core networks.

DiffServ is based on bits marking in the IP packet/Ethernet Frame headers. The traffic shall be marked as close to the source as possible, then it could be policed, shaped and queued throughout the networks till the recipient of the packet. Differentiated services are usually statically configured on the network nodes, have no signaling overhead and could be met in all kinds of networks: ISP, Telecoms, Mobile, Cable and even Enterprise still use them today.

Dynamic QoS enables per service and per subscriber level QoS rule setting. There are several approaches for implementing Dynamic QoS in Service provider networks. 3GPP adapted the Diameter protocol with QoS extension in the Policy Control and Charging (PCC) function.

Diameter QoS application runs between a network element (NE) acting as a Diameter Client, and the resource Authorization Entity (AE), acting as a Diameter Server. Figure 62 present the high-level picture of the QoS authorization architecture using the Diameter QoS application.

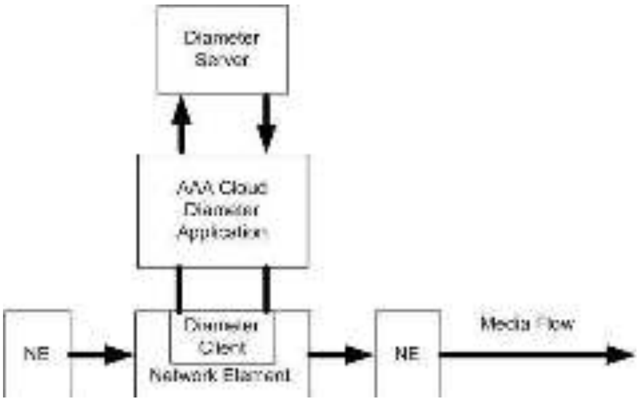


Figure 62 - Architecture for Diameter QoS Application [2].

There are three different categories of endpoints:

- Category 1: Application endpoint has no QoS control capability neither on application nor on network level
- Category 2: Application endpoint has QoS control capability on application level (e.g. SIP signaling)
- Category 3: Application endpoint has QoS control capability at the network level, i.e., sets up connection on application level, and translates service characteristics to network level QoS requirements locally, and requests the resources through network signaling (e.g., Resource reservation protocol (RSVP) or link-specific protocol)

The diversity of QoS capabilities of endpoints and QoS schemes of network technology leads to the distinction on the interaction mode between the QoS authorization system and underlying NEs. When the IntServ scheme is employed by a Category 3 endpoint, the authorization process is typically initiated by an

NE when a trigger is received from the endpoint such as network QoS signaling. In the Diffserv scheme, since the NE is unable to request the resource authorization on its own initiative, the authorization process is typically triggered by either the request of Application endpoint or policies defined by the operator.

As a consequence, two interaction modes are needed in support of different combinations of QoS schemes and endpoint's QoS capabilities: Push mode and Pull mode.

B.4.1.1 Push mode

The QoS authorization process is triggered by the Application server or by local network conditions (e.g., time of day on resource usage and QoS classes), and the authorization decisions are installed by the AE to the network element on its own initiative without explicit request. In order to support Push mode, the AE (i.e., Diameter server) should be able to initiate a Diameter authorization session to communicate with the NE (i.e., Diameter client) without any pre-established connection from the network element.

B.4.1.2 Pull mode

The QoS authorization process is triggered by the network signaling received from end-user equipment or by a local event in the NE according to pre-configured policies, and authorization decisions are produced upon the request of the NE. In order to support Pull mode, the NE (i.e., Diameter client) will initiate a Diameter authorization session to communicate with the Authorizing Entity (i.e., Diameter server). For Category 1 and 2 Application endpoints, Push mode is required.

For a Category 3 Application endpoint, either Push mode or Pull mode may be used. Push mode is applicable to certain networks, for example, Cable network, DSL, Ethernet, and Diffserv-enabled IP/MPLS. Pull mode is more appropriate to IntServ-enabled IP networks or certain wireless networks such as the General Packet Radio Service (GPRS) networks defined by the Third Generation Partnership Project (3GPP). Some networks (for example, Worldwide Interoperability for Microwave Access (WiMAX)) may require both Push and Pull modes.

B.4.2 PCC architecture

Figure 63 presents the PCC architecture.

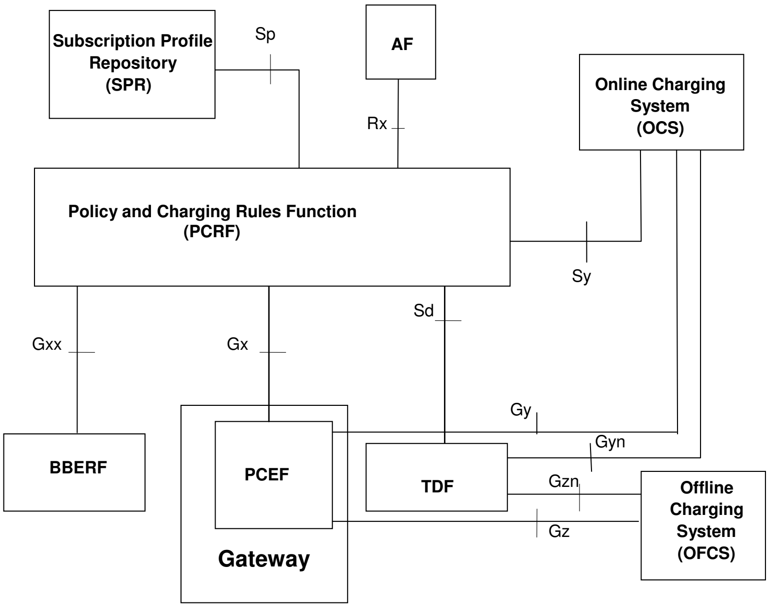

Subscription Profile Repository (SPR)
Sp
AF
Rx
Online Charging System (OCS)
Policy and Charging Rules Function (PCRF)
Sy
Sd
Gxx
Gx
Gy
Gyn
BBERF
PCEF
TDF
Gzn
Gz
Offline Charging System (OFCS)
Gateway

Figure 63 - Overall PCC logical architecture (non-roaming, SPR is used) [3].

The elements related to Policy control are the following:

- Application Function (AF): the AF interacts with services that require dynamic PCC. E.g., in case of IMS, AF is the P-CSCF. The AF extracts session information (e.g., from Service Description Protocol field), and sends the information to PCRF over the Rx interface. Such information includes, but is not limited to:
  - IP filter information to identify the service data flow for policy control and/or differentiated charging;
  - Media/application bandwidth requirements for QoS control.

  In addition, for sponsored data connectivity:
  - the sponsor's identification,

  - optionally, a usage threshold and whether the PCRF reports these events to the AF,
  - information identifying the application service provider and application (e.g. SDFs, application identifier, etc.).

  The AF can also subscribe at the PCRF to the notification of events in the network, such as IP session termination or access technology type change.

- Subscription Profile Repository: provides user specific policies and data over the Sp interface.
- Policy and Charging Rules Function (PCRF): it receives session information on Rx, subscriber specific policies over Sp, access network information over Gx, or if BBERF is used, than over Gxa/Gxc. Operators can configure policies in the PCRF, which must applied to given services. Based on those information it brings service-session level policy decisions and provides them to PCEF and optionally to BBERF. PCRF also sends event reports from PCEF and optionally the BBERF to the AF, e.g., for video/audio codec adaptation.
- Policy Control Enforcement Function (PCEF): enforces policy decisions based on the PCC rules provided by PCRF over the Gx interface. It may perform measurements of user plane traffic (e.g., data volume, session duration). It reports the usage of resources for offline charging and interacts with online charging.
- Bearer Binding and Event Reporting Function (BBERF) is required if no on-path QoS negotiation is available (by GTPv2-C), and DSMIPv6/IPsec or PMIP/IP GRE tunnels are used between the P-GW and the access GW of the UE, not capable of implementing QoS bearers for the services of the UEs. BBERF is responsible for bearer binding and QoS enforcement based on QoS rules provided by the PCRF over the Gxa/Gxc interface. Furthermore it is responsible for event reporting towards the PCRF, about access network type, bearer state and other information.

Policy control comprises gating control and QoS control. Gating control is applied by the PCEF on a per service data flow basis.

B.4.2.1 PCC rule (PCEF) vs QoS rule (BBERF)

The Policy Control and Charging rule (PCC rule) comprises the information that is required to enable the user plane detection of, the policy control and proper charging for a service data flow. The packets detected by applying the service data flow template of a PCC rule are designated a service data flow.

Two different types of PCC rules exist: dynamic PCC rules and pre-defined PCC rules. The dynamic PCC rules are provisioned by the PCRF via the Gx reference point. Pre-defined PCC rules are directly provisioned into the PCEF and only referenced by the PCRF. While packet filters in a dynamic PCC rule are limited to the five tuple of source and destination IP, source destination port, transport protocol, and some more header fields, the pre-defined PCC rules may use DPI filters for more fine-grained flow detection, charging control. Those filters are not standardized by 3GPP. Appendix B.6 presents the main elements of a dynamic PCC rule. TS 23.203 [3] contains more details on PCC rules. There are both mandatory and conditional fields, denoted in Appendix B.6.

In case of off-path QoS control, PCRF needs to provide QoS information to the BBERF via the Gxa/Gxc reference points. QoS rule includes only a subset of PCC rule, but with the same service-level granularity. It includes hence typically the filter information (SDF template, precedence), QoS parameters (e.g., QCI, bit rates), but not charging-related information.

B.4.2.2 Network-initiated and UE-initiated QoS control

For services provided by the access provider, such as IMS voice, mobile TV etc., the network-initiated QoS control procedure is preferable. For service that are not known by the operator, UE-initiated QoS control is possible.

A network-intiated QoS control procedure may have the following steps:

6. Application level signaling between the UE and the AF (e.g., SIP, SDP)
7. Session information provision from the AF to the PCRF (over the Rx reference point). In case of IMS services, the SDP information is mapped to QoS information, such as bitrate, service type
8. The PCRF may request subscriber-related information from the SPR
9. PCRF makes policy decision based on session information, operator-defined service policies, subscription information and generates PCC / QoS rules
10. PCC rules are pushed by the PCRF to the PCEF and PCEF enforces the policy and charging rules, and, conditionally, if BBERF is required, then QoS rules are pushed to the BBREF and installed.

An UE-initiated QoS control procedure may have the following steps:

1. Application level signaling between the UE and the AF (e.g., SIP, SDP)

2. Session information provision from the AF to the PCRF (over the Rx reference point). In case of IMS services, the SDP information is mapped to QoS information.
3. The PCRF may request subscriber-related information from the SPR.
4. The application on the UE side makes request through vendor-specific APIs for the access interface, to request the needed QoS resources.
5. UE sends resource request, including QoS class, packet filters for the service. In E-UTRAN that is called UE-requested bearer resource modification. In GERAN/UTRAN, it is realized by secondary PDP context activation/modification
6. If BBERF exists, it initiates PCRF interaction over GXa/Gxc interface. If there is no BBERF, the PCEF initiates PCRF interaction over Gx interface.
7. Same as step 4 in network-initiated case.
8. Same as step 5 in network-initiated case.

B.5 Characteristics of standardized QCI values

Table 1 - Standardized QCI characteristics (see TS 23.203 [3] for details)

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100 ms	1E-2	Conversational Voice
2		4	150 ms	1E-3	Conversational Video (Live Streaming)
3		3	50 ms	1E-3	Real Time Gaming
4		5	300 ms	1E-6	Non-Conversational Video (Buffered Streaming)
5	Non-GBR	1	100 ms	1E-6	IMS Signalling
6		6	300 ms	1E-6	Video (Buffered Streaming), TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) for Multimedia Priority Service subscribers
7		7	100 ms	1E-3	Voice, Video (Live Streaming), Interactive Gaming
8		8	300 ms	1E-6	same as for QCI=6, for premium subscribers
9		9	300 ms	1E-6	same as for QCI=6, for non-privileged subscribers

B.6 Elements of a dynamic PCC rule

Table 2 – Elements of a dynamic PCC rule.

Information name	Description	Presence of field in QoS rule
Rule identifier	Uniquely identifies the PCC rule, within an IP-CAN session. It is used between PCRF and PCEF for referencing PCC rules.	X
	Service data flow detection	
Precedence	Determines the order, in which the service data flow templates are applied at service data flow detection, enforcement and charging.	X
Service data flow template	Either a list of service data flow filters or an application identifier that references the corresponding application detection filter for the detection of the service data flow.	X
	Charging	
Charging key	The charging system (OCS or OFCS) uses the charging key to determine the tariff to apply to the service data flow.	
Service identifier	The identity of the service or service component the service data flow in a rule relates to.	
Sponsor Identifier	An identifier, provided from the AF which identifies the Sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes.	
Application Service Provider Identifier	An identifier, provided from the AF which identifies the Application Service Provider, used for sponsored flows to correlate measurements from different users for accounting purposes.	
Charging method	Indicates the required charging method for the PCC rule. Values: online, offline or neither.	
Measurement method	Indicates whether the service data flow data volume, duration, combined volume/duration or event shall be measured. This is applicable to reporting, if the charging method is online or offline. Note: Event based charging is only applicable to predefined PCC rules and PCC rules used for application detection filter (i.e. with an application identifier).	
Application Function Record Information	An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports.	

Information name	Description	Presence of field in QoS rule
Service identifier level reporting	Indicates that separate usage reports shall be generated for this Service identifier. Values: mandated or not required	
Policy control		
Gate status	The gate status indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed) at the PCEF.	
QoS class identifier	Identifier for the authorized QoS parameters for the service data flow.	X
UL-maximum bitrate	The uplink maximum bitrate authorized for the service data flow	X
DL-maximum bitrate	The downlink maximum bitrate authorized for the service data flow	X
UL-guaranteed bitrate	The uplink guaranteed bitrate authorized for the service data flow	X
DL-guaranteed bitrate	The downlink guaranteed bitrate authorized for the service data flow	X
Redirect	Redirect state of the service data flow (enabled/disabled)	
Redirect Destination	Controlled Address to which the service data flow is redirected when redirect is enabled	
ARP	The Allocation and Retention Priority for the service data flow consisting of the priority level, the pre-emption capability and the pre-emption vulnerability	X
PS to CS session continuity	Indicates whether the service data flow is a candidate for vSRVCC.	X
Access Network Information Reporting		
User Location Report	The serving cell of the UE is to be reported. When the corresponding bearer is deactivated, and if available, information on when the UE was last known to be in that location is also to be reported.	X
UE Timezone Report	The time zone of the UE is to be reported.	X
Usage Monitoring Control		
Monitoring key	The PCRF uses the monitoring key to group services that share a common allowed usage.	