

Project Number:	CELTIC / CP7-011
Project Title:	<u>M</u> obile Networks <u>E</u> volution for <u>I</u> ndividual <u>C</u> ommunications Experience – MEVICO
Document Type:	P

Document Identifier:	D 4.3.2
Document Title:	Final Design of the MEVICO Traffic Engineering Architecture
Source Activity:	WP4
Main Editor:	Ece Saygun
Authors:	See the Authors section
Status / Version:	1.00
Date Last changes:	28.02.2013
File Name:	D 4.3.2

Abstract:	In this document the final traffic engineering architecture of MEVICO designed for EPC with the integration framework are described based on research completed. Validation results, especially the ones relating to the proposed architecture are included. For more details on validations Please see D 4.4.1. Also D 4.3.1 would be a good introductory reading since state of the art and a wider area of research topics are included in it.
-----------	---

Keywords:	QoS, traffic management, traffic engineering, scenarios, QoE, architecture
-----------	--

Document History (most recent):	
28/02/13	Ericsson Turkey did overall editing
21/12/12	ALU added Appendix 2.1
21/12/12.	ALU finished 3.4.2 and 5.2.5.4
20/12/12	Ericsson Turkey updated Section 4.1
19/12/12	AVEA updates Section 4.2
18/12/12	ALU on 3.4.2 and 5.2.5.4
18/12/2012	BME-MIK updates Section 6
17/12/2012	TUB updates to Section 3.4.3
14/12/2012	CUT contribution section 4.1.2
12/12/2012	NSN update
11/12/2012	BME-MIK updated section 3.4
10/12/2012	Montimage updated section 4.1.1

Table of Contents

Table of Contents	2
Authors	5
Executive Summary	8
List of acronyms and abbreviations	9
1 Introduction	12
2 Traffic engineering building blocks	13
3 Macroscopic traffic management	15
3.1 Access technology reselection	15
3.2 Advanced offloading techniques.....	15
3.2.1 Fine grained network-based mobility management: NB-IFOM	15
3.2.2 QoE-aware Traffic Engineered Handovers.....	25
3.2.3 Support of multipath flows	28
3.3 Multi-Criteria cell selection	30
3.3.1 Multi-criteria Cell Selection Algorithms	32
3.3.2 Summary of Evaluation Results.....	33
4 Microscopic traffic management	34
4.1 QoS differentiation based on applications and user profiles	34
4.1.1 Application and user classification	34
4.1.2 Application and user based differentiation	45
4.2 End-to-end QoS	53
4.2.1 End-to-end (E2E) QoS in 3G.....	53
4.2.2 Services, KPIs and implementation steps for E2E QoS parameters in the network	53
5 Improved resource selection & caching	58
5.1 Resource selection	58
5.2 Internet-based Content Distribution via CDN and P2P Overlays	58
Following topics have been detailed in D 4.3.1:	58
5.2.1 ALTO extension proposal for UE with scarce resources and/or intermittent connection.....	58
5.3 P4P	61
5.3.1 BitTorrent Protocol.....	61
5.3.2 Proposed Network Model	62
5.3.3 Summary of Evaluation Results.....	64
6 Integration of technologies	65
6.1 ALTO.....	66
6.2 NB-IFOM.....	68
6.3 MCCS	69
6.4 Selection of HO candidates in Wi-Fi hotspots	69
6.5 GW selection.....	70

6.6	Bulk Traffic Analysis.....	71
6.7	Deep Packet Inspection.....	72
6.8	QoE estimation and traffic manipulation.....	72
6.9	MPTCP-PR.....	73
6.10	mP4P.....	74
7	Conclusions	76
	Acknowledgement.....	77
	References	78
1	Appendix: IETF standardization on traffic management.....	88
1.1	IETF ALTO protocol in a 3GPP study item on IMS based P2P.....	88
1.1.1	Integration of ALTO in the IMS P2P Content Distribution Service.....	88
1.1.2	Status	89
1.2	Relevance for Mevico WP4	90
2	Appendix: 3GPP standardization on traffic management	91
2.1	SAE Network Architecture.....	91
2.1.1	Introduction.....	91
2.1.2	Non-Roaming Architecture.....	91
2.1.3	Roaming Architecture (home routed).....	93
2.1.4	Roaming Architecture (local breakout).....	94
2.1.5	Relevance for MEVICO WP4	95
2.2	QoS and EPS Bearers.....	95
2.2.1	Session and Bearer Management.....	95
2.2.2	QoS Concept.....	95
2.2.3	Characteristics of an EPS bearer.....	96
2.2.4	Relevance for MEVICO WP4	98
2.3	Policy and Charging Control (PCC)	98
2.3.1	Architecture	98
2.3.2	Basic features and operations.....	99
2.3.3	Application detection and control.....	102
2.3.4	Relevance for MEVICO WP4	102
2.4	Voice Support in LTE.....	102
2.4.1	Overview.....	102
2.4.2	IMS	102
2.4.3	CS Fallback.....	115
2.4.4	Single Radio Voice Call Continuity.....	116
2.4.5	Relevance for MEVICO WP4	117
2.5	Traffic Offloading to WLAN.....	118
2.5.1	Offload per PDN Connection.....	118
2.5.2	IP Flow Mobility and Seamless WLAN Offload.....	118
2.5.3	Non-Seamless WLAN offload.....	119
2.5.4	The Access Network Discovery and Selection Function (ANDSF)	119
2.5.5	Relevance for MEVICO WP4	120
2.6	Service identification for improved radio utilization for GERAN (SIRIG).....	121
2.6.1	Overview.....	121
2.6.2	Motivating use cases.....	121

2.6.3	Solution Overview	121
2.6.4	Open Issues likely to be addressed in future work:.....	121
2.6.5	Relevance for MEVICO WP4	122
2.7	User Plane Congestion Management (UPCON)	122
2.7.1	Overview.....	122
2.7.2	Status in 3GPP	122
2.7.3	Some Considered Use Cases.....	122
2.7.4	Requirements	123
2.7.5	Key issues investigated in Stage 2 Study.....	123
2.7.6	Relevance for MEVICO WP4	124
2.8	Abbreviations	125

Authors

Partner	Name	Phone / Fax / e-mail
Nokia Siemens Networks		
	Dr. Thomas Belling	Phone: + 49 89 5159 35207 e-mail: Thomas.Belling@nsn.com
	Christian Ruppelt	Phone: + 49 89 5159 39125 e-mail: christian.ruppelt@nsn.com
	Wolfgang Hahn	Phone : e-mail: wolfgang.hahn@nsn.com
Technical University of Chemnitz		
	Thomas Bauschert	Phone: e-mail: thomas.bauschert@etit.tu-chemnitz.de
	Gerd Windisch	Phone: e-mail: gerd.windisch@etit.tu-chemnitz.de
Deutsche Telekom		
	Gerhard Hasslinger	Phone: e-mail: Gerhard.Hasslinger@telekom.de
T-Systems		
	Anne Schwahn	Phone: e-mail: anne.schwahn@t-systems.com

Technical University Berlin

Lukasz Budzisz

Phone:

e-mail: lukasz.budzisz@tu-berlin.de

Sven Wiethoelter

Phone:

e-mail: wiethoel@tkn.tu-berlin.de

Berthold Rathke

Phone:

e-mail: rathke@tkn.tu-berlin.de

Tacettin Ayar

Phone:

e-mail: ayar@tkn.tu-berlin.de

Budapest University of Technology and Economics – Mobile Innovation Centre

László Bokor

Phone:

e-mail: bokorl@hit.bme.hu

Zoltán Faigl

Phone:

e-mail: zfaigl@mik.bme.hu

József Kovács

Phone:

e-mail: josephus@josephus.hu

University of Vienna

Florian Metzger

Phone:

e-mail: florian.metzger@univie.ac.at

Albert Rafetseder

Phone:

e-mail: albert.rafetseder@univie.ac.at

Ericsson Turkey

Ece Saygun

Phone:

e-mail: ece.saygun@ericsson.com

Turk Telekom	
Ahmet Serdar Tan	Phone: e-mail: ahmetserdar.tan@turktelekom.com.tr

VTT	
Tapio Suihko	Phone: e-mail: Tapio.Suihko@vtt.fi

Alcatel Lucent	
Sabine Randriamasy	Phone: e-mail: Sabine.Randriamasy@alcatel-lucent.com

Montimage	
Bachar Wehbi	Phone: e-mail: bachar.wehbi@montimage.com

AVEA	
Engin ZEYDAN	Phone: e-mail: engin.zeydan@avea.com.tr
Çağatay EDEMEN	Phone: e-mail: cagatay.edemen@avea.com.tr
Salih Ergüt	Phone: e-mail: salih.ergut@avea.com.tr

Executive Summary

As mobile and wireless communication networks move toward broadband converged networks and applications, the demands on the infrastructure will increase tremendously. The MEVICO project aimed at identification of the technologies for the evolution of 3GPP LTE-mobile broadband network. The target was to innovate and develop new network concepts for meeting the future requirements of the evolving mobile networks and usage. The work related to this document encompasses the smart traffic management techniques on which the MEVICO partners have focused on. Each partner has focused on the technologies according to their research plans and their results have been presented in this document.

This document follows the categorization logic, which is the traffic engineering building blocks, in order to group different techniques.

Using these building blocks, various mechanisms have been categorized according to common functionality or solution space. Since this project focused on innovative approaches on packet core, mobile backhaul and operator service domain, the radio management aspects have not been taken into consideration. The same applies to traffic management, which is restricted to the application layer or is mainly about business modelling aspects. The four building blocks of highest interest to the project consortium are ‘microscopic traffic management’, ‘macroscopic traffic management’, ‘improved resource selection and caching’ and ‘deployment of new network resources’. ‘Deployment of new network resources’ has not been handled in this document.

In this document the traffic engineering architecture has been proposed based on research completed.

List of acronyms and abbreviations

2G/3G/4G	2nd/3rd/4th Generation Cellular Mobile Phone System (GSM, UMTS, LTE,...)
3GPP	3rd Generation Partnership Project, based on GSM Technology
3GPP	3rd Generation Partnership Project 2, based on GSM Technology
AC	Application Client
ALTO	Application Layer Traffic Optimization
AMBR	Aggregated Maximum Bit Rate
API	Application Programming Interface
APN	Access Point Name
ARP	Allocation and Retention Priority
ARQ	Automatic Repeat Request
AS	Autonomous System
AVP	Active Virtual Peer
BNG	Broadband Network Gateway
BS	Base Station
CAPEX	Capital Expenditure
CDN	Content Distribution Network
CIF	Common Intermediate Format
CSCF	Call Session Control Function
CSP	Communication Service Provider
DHT	Distributed Hash Table
DL	Downlink
DNS	Domain Name System
DoA	Direction of Arrival
DPI	Deep Packet Inspection
DSL	Digital Subscriber Line
DSMIPv6	Dual Stack Mobile IPv6
e2e	End to end
ECMP	Equal Cost Multi-Path
eNB	eNodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved UTRAN
FTP	File Transfer Protocol
GAN	Generic Access Network
GBR	Guaranteed Bit Rate
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GW	Gateway
HA	Home Agent
HeNB	Home eNodeB
HLR	Home Location Register
HO	Handover
HSS	Home Subscriber Server
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
IMPEX	Implementation Expenditure

IMS	IP Multimedia Subsystem
ISP	Internet Service Provider
LAN	Local Area Network
L-GW	Local Gateway
LIPA	Local IP Access
LTE	Long Term Evolution
LTE-A	LTE-Advanced
MAC	Medium Access Control
MacTM	Macroscopic Traffic Management
MAPCON	Multi-Access PDN CONnectivity
MBR	Maximum Bit Rate
MicTM	Microscopic Traffic Management
MIH	Media Independent Handover
MME	Mobility Management Entity
MNO	Mobile Network Operator
MP2MP	Multipoint-to-Multipoint
MPLS	Multiprotocol Label Switching
MPTCP	Multi-Path TCP
MT	Mobile Terminal
MWR	Microwave Radio
NAPTR	Naming Authority Pointer [Resource Record]
NAS	Non Access Stratum
NAT	Network Address Translation
NB-IFOM	Network Based IP Flow Mobility
NE	Network Element
NIC	Network Interface Card
OAM	Operation, Administration, and Maintenance
OPEX	Operational Expenditure
OSPF	Open Shortest Path First
P2P	Peer-to-Peer
P2MP	Point-to-Multipoint
P4P	Provider Portal for (P2P) Applications
PCC	Policy and Charging Control
PCE	Path Computation Element
PCP	Priority Code Point
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDP	Packet Data Protocol
P-GW	PDN Gateway
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request For Comments
RNC	Radio Network Controller
RNL	Radio Network Layer
RRM	Radio Resource Management
RTSP	Real Time Streaming Protocol
SCADA	Supervisory Control And Data Acquisition
SCTP	Stream Control Transmission Protocol
SeGW	Security Gateway
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway

SIP	Session Initiation Protocol
SIPTO	Selected IP Traffic Offload
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SRV	Service [Location Resource Record]
TAI	Tracking Area Identity
TCP	Transmission Control Protocol
TE	Traffic Engineering
TNL	Transport Network Layer
UDP	User Datagram Protocol
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
UTRAN	UMTS Terrestrial Radio Access Network
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network

1 Introduction

The research project MEVICO has investigated aspects of the 3GPP LTE-mobile broadband network for its evolution in the mid-term in 2011-2014 and beyond. The goal was to contribute to the technical drive and leadership of the Evolved Packet Core (EPC) network of the 3GPP, and thus support the European industry to maintain and extend its strong technical and market position in the mobile networks market. The project followed an end-to-end system approach on evolution of the EPC. The focus has been on the connectivity layers of the system, for example on the part of the future LTE network which provides the efficient packet transport and mobility support for the applications & end-user services accessed over the LTE and LTE-Advanced radio systems. The technical research areas of the project have covered relevant topics in the areas of network architecture, mobility & routing, packet transport, traffic management, network management & engineering and techno-economic aspects. The project has included both conceptual research and demo/trial system implementations.

This is the final document of the end-to-end (e2e) QoS and Traffic Engineering Architecture task in MEVICO. Here traffic engineering techniques which fall only in the research interests of the partners and which have been finalized are being described. The state of the art at the start of the MEVICO project has been described in detail in D 4.3.1 and in D 4.3.2 this is followed by proposed improvements and new technologies in line with the research progress.

A wide coverage of potential improvements on top of state of the art have been included in D 4.3.2 however only some of these have been researched and have produced results.

Some techniques which have been mentioned in D 4.3.1 but there has not been any updates prior to D 4.3.2 are as follows:

- Selection of core network elements
- Change of routing within backhaul
- Cross Layer Interference Detection
- QoS support for external content
- Selective admission control
- Resource selection and re-direction mechanisms

Finalized work on research topics is followed by a section on Integration where the placement of the technology in the MEVICO architecture and potential overlaps with other proposed techniques has been described.

2 Traffic engineering building blocks

The building blocks described in this section provide an overview about the mechanisms introduced in the MEVICO deliverable D 4.2.1 to improve quality of experience for the user and to enable efficient usage of infrastructure and IT resources. For the latter there is a benefit for other stakeholders in the (mobile) communication business, such as communication service providers (e.g. MNO), content providers and CDN providers. We have identified six different categories, which can be used to assign the various building blocks and aspects. Figure 2-1 displays the principal building blocks for traffic management with some given examples. There are three blocks which may be correlated with each other similar like lower layer functions provide services to higher layer functions in a communication stack.

The building blocks have been detailed in D 4.2.1. In this document, only the topics that fall in the MEVICO partners' research areas and where there is finalized research have been covered.



Figure 2-1: Building blocks of traffic engineering mechanisms

In the current case microscopic traffic management (MicTM) may provide services to macroscopic traffic management (MacTM). MicTM includes flow specific mechanisms, e.g. to improve quality of experience for the user. MacTM deals with the manipulation of routes through the networks, e.g. to improve efficient usage of resources. In addition to microscopic and macroscopic traffic management, a third group addresses the selection of resources in conjunction with caching, if necessary. This building block may rely on services of both microscopic and macroscopic traffic management. A resource in this context is associated with specific (multi-media) content, which is requested by users. All the above mentioned categories are associated with mechanisms that may require support from lower layers (below application). In addition we have identified two more building blocks which may require only little or no support from lower layers. These could be in place without dependence on other traffic management building blocks. On one hand there is application supported traffic management. There are many applications based on CDN and P2P, which try to optimize performance from end user perspective without getting support from network elements. Another building block has been identified, which is more relevant from business perspective without too many technical aspects. Mainly network operators but possibly other stakeholders as well may influence user behaviour by defining certain constraints for usage of networks / services and certain incentive to comply with the usage constraints. Deployment of new network resources is identified as the last building block in this construction. It should be noted that it is very hard to totally separate these building blocks, there is certainly overlap among them. These overlaps have been addressed in Section 6, the Integration section.

For the purpose of scenario definition we want to introduce a simplified role model in order to understand the challenges, problems and requirements associated with the different stakeholders. These are the following:

- End user
- Communication service provider (CSP) – with a special viewpoint on mobile operators

- CDN Provider – usually a company with large amount of infrastructure to distribute content as close as possible to the end user. Customer is usually the content provider.
- Application / content provider – commercial or non-commercial entity, which inserts content for global or limited use in the Internet.

The roles of CSP, CDN Provider and content provider could be intertwined. For example, Google provides content but also has deployed a huge infrastructure to deliver it to the end user. On the other hand there are some operators, which want to make additional business by deploying CDN infrastructure or provide services via “walled-garden” models. This way end users should be motivated to connect to resources within the CSP or associated domains.

3 Macroscopic traffic management

This section proposes algorithms and mechanisms for macroscopic traffic management, in the areas of intra- and inter-technology cell (re)selection, selection of core network elements, traffic offloading, and cross-layer interference detection.

3.1 Access technology reselection

The topic of access technology reselection has been detailed in D 4.3.1.

3.2 Advanced offloading techniques

3.2.1 Fine grained network-based mobility management: NB-IFOM

3.2.1.1 What is IFOM?

IP Flow Mobility (3GPP TS 23.261, 3GPP TR 23.861) has been designed to selectively assign traffic flows of user equipment (UE) to separate radio access networks representing different technologies. It provides simultaneous attachment to overlapping radio coverage while allowing fine granularity of IP flow mobility between access networks, hereby allowing network operators to optimize load among alternate access technologies. The technique depends on the presence of mobility aware network protocols such as DSMIPv6, PMIPv6 with flow bindings. One of the main disadvantages of IFOM is that the current IFOM standardization is based on DSMIPv6 and it also relies on the mobile terminals to provide the flow routing policy as part of the DSMIPv6 mobility signaling (Binding Update) to the PDN Gateway (Home Agent). When an operator wants to initiate a change in flow routing, the current solution relies on the Access Network Discovery and Selection Function (ANDSF) as specified in 3GPP TS 23.402:

- First the UE registers with an ANDSF server to receive access network information and operator preferences with regard to the selection of an access network.
- Then the ANDSF service will notify individual UEs about updated flow routing policies.
- UE sends a DSMIPv6 Binding Update (HoA, CoA, Lifetime, BID, FID, flow description) message to the PDN-GW (HA) together with the requested routing rules via the FID mobility option with both the routing filters and the BID.
- The PDN GW sends an IP-CAN session modification request to the PCRF providing the updated routing rules to the PCRF. The PCRF stores the updated mapping between routing addresses and SDFs.
- The PCRF sends an acknowledgement to the PDN GW, including updated PCC rules if appropriate.
- The HA sends a Binding Acknowledgment (Lifetime, HoA, BID, FID) to indicate which routing rules requested by the UE are accepted.
- Finally, the PCRF ensures the relevant QoS rules and/or releases resources that were moved away.

The procedure to change flow policies is very UE centric, as the operator firstly delivers the routing policies to the UE, and then the UE must provide these policies to the Home Agent (PDN Gateway). The ANDSF has no interface to the PCC system, therefore it requires other ways to get informed about the updated flow policies for a particular UE. Based on these operational properties we conclude that dynamic and network initiated changes in the IP flow routing policies of UEs are difficult. Furthermore, in the current standard it is possible that the network context and resource availability may have changed by the time the UE provides the routing policies to the network, therefore the PCRF will not be able to authorize the new flow policies anymore.

3.2.1.2 Network Based IFOM (NB-IFOM)

In order to overcome the shortcomings of IFOM we propose a solution to allow dynamic management of IP flow routing policies issued by the operator. The architecture builds on top of an IETF proposal which introduces Home Agent initiated flow bindings into Mobile IPv6 signalling. The multiple care-of address registration extension of the Mobile IPv6 protocol makes it possible to use multiple egress interfaces and

operate policy based routing using these interfaces by the flow binding mechanism specified in RFC6089. The document describes that in order to initiate a flow binding operation a valid Mobile IPv6 binding is required. Similarly to that technique a HA initiated flow binding operates via the Flow Binding Indication (FBI) and the Flow Binding Acknowledgement (FBA) messages, where the latter is used for the acknowledgement of the FBI message. By relying on the basic concepts introduced by the soon to be RFCd HA initiated flow binding proposal we extended the functionality of the model by defining monitoring points for traffic state and analysis overall the network and adding policy servers to manage the monitoring points and enforce policies based on the processed data.

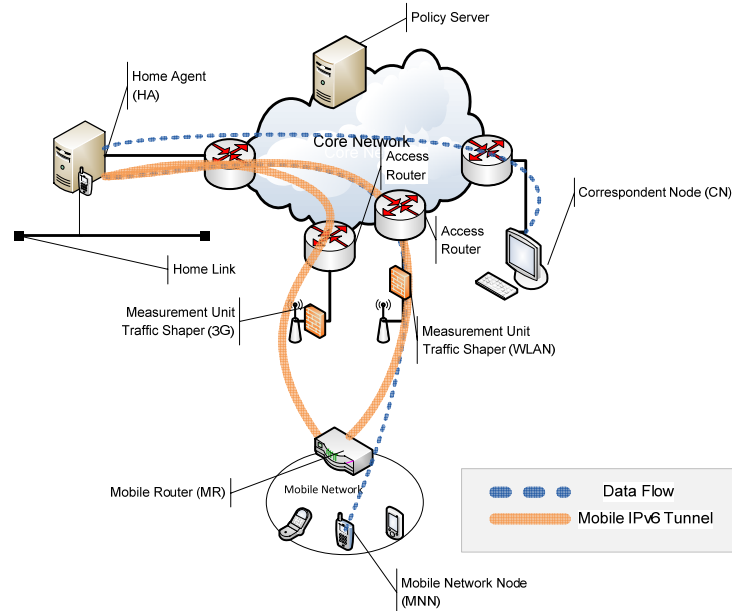


Figure 3-1: NB-IFOM network architecture

In order to perform network based flow-mobility operations the existing Mobile IPv6 (NEMO/MCoA) architecture must be extended with the following special nodes (Figure 3-1):

Measurement Unit: One or more DPI capable (Deep Packet Inspection) devices throughout the core network. They passively monitor the overall and flow based network usage statistics for a given link. When DPI is not available, i.e., when the tunneled traffic is encrypted, it reports only aggregated statistics on a given link.

Mobile Node/Router (MN/MR): Mobile IPv6 node with extended functionalities. Performs and policy routing and flow binding based on network events. Such policies received from the Mobile IPv6 network management entity (Home Agent) are always overrule the local decisions and predefined settings.

Home Agent (HA): Mobile IPv6 central management entity with extended functionality. Relays and enforces network-based policies received from the Policy Server. Synchronizes its Binding Cache to the Policy Server.

Policy Server (PS) (PCRF): A central entity which performs network-based policy binding based on overall network parameters. It receives link and flow usage information from multiple Measurement Units and maintains an aggregated Binding Cache from multiple Home Agents. Knowing the actual flow binding usage on the network it activates policies when trigger conditions are met.

NB-IFOM enables operators to enforce IP flow routing policies in the downlink without involving the UE first. It provides a way to the PCRF (the central policy control entity) to decide on the flow routing policy based on e.g., the available resources in the network, before signaling the policies to the UE. This is more efficient, than solutions that rely on the UE to provide the routing policies to the network first, before they are authorized by the PCRF.

3.2.1.2.1 Use-cases

Default Flow Binding Provisioning is used for example in an environment where a central entity wants to force Service Level Agreements (SLA) to a customer, e.g., forcing P2P traffic through WiFi while allowing UMTS access for HTTP traffic.

The Traffic Offloading technique makes it possible to move certain data flows from one interface to another, e.g., in case of increasing traffic load in 3G segment move video streams to the WiFi segment.

Policies can be much complex based on the fact that the core network entities know about their actual traffic conditions.

Flow Binding Revocation is useful when due to an administrative decision, a certain flow binding is no longer valid for the MN.

3.2.1.2.2 Protocol specification

3.2.1.2.2.1 Policy Server communication

The following figure represents the relation between communication nodes and the Policy server.

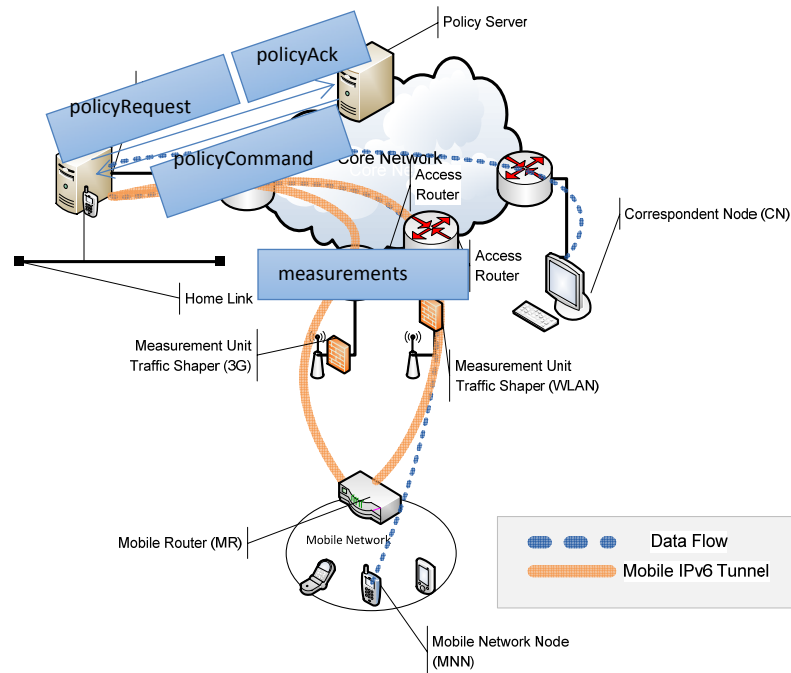


Figure 3-2: Communication with the Policy Server

3.2.1.2.2.2 Measurements

Measurement nodes are periodically reporting towards the Policy Server. The messages are not acknowledged; therefore policy management operation must not depend on continuous reports.

The protocol may report overall statistics along with usage statistics of several flows. Flows are predefined and correspond to the flows defined on the Policy Server.

Protocol transport	TCP
Protocol format	XML
Protocol fields	entity (flow id, link), bandwidth, packet loss, latency

3.2.1.2.2.3 policyRequest

The message is sent from the Home Agent to the Policy Server. HA requests new policies from the PS for a given Binding entry (HoA, BID, CoA triplet) when the Binding Cache Entry is changed on the HA.

Protocol transport	UDP
Protocol format	XML or JSON
Protocol fields	HoA, BID, CoA, optional flags

3.2.1.2.2.4 policyCommand

The Policy Server may send a policyCommand message to the Home Agent, indicating the applicable flow policies on the Home Agent.

Protocol transport	UDP
Protocol format	XML or JSON
Protocol fields	Task ID, Flow descriptor, BID, HoA

– Binding Update (Binding Acknowledgement)

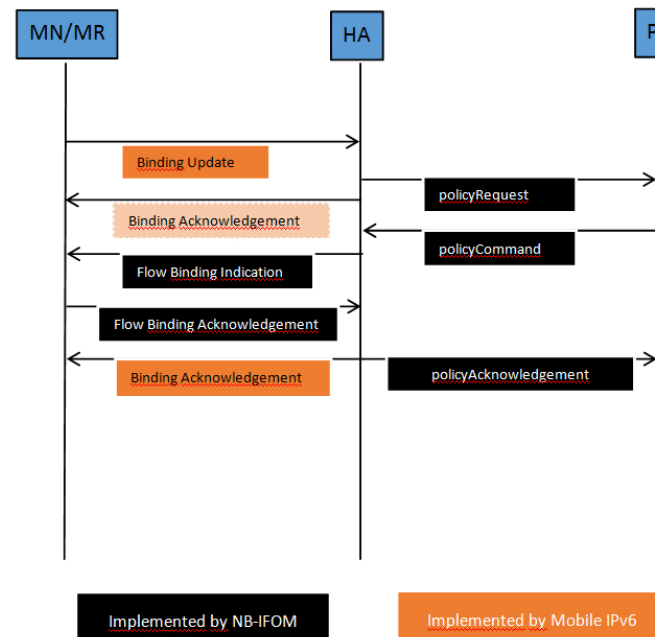


Figure 3-4: Complete message flow of NB-IFOM

3.2.1.3 NB-IFOM implementation details

3.2.1.3.1 Policy Server

The Policy Server has been implemented in Ruby as a multi-threaded background service running on UNIX/Linux platform. It uses the native socket and TCP/IP interface provided by the operating system. Ruby was chosen to enable a more agile development methodology and quick prototyping of applications as the specification evolves.

As the Policy Server node has to store quite extensive set of data structures, an external RDBMS is used to better visualize and organize data. The chosen solution was MySQL with InnoDB storage engine which supports foreign keys in order to maintain coherency throughout the data tables. The database is replicable therefore scalability of the Policy Server node is easily achievable to reduce single point of failures in the architecture.

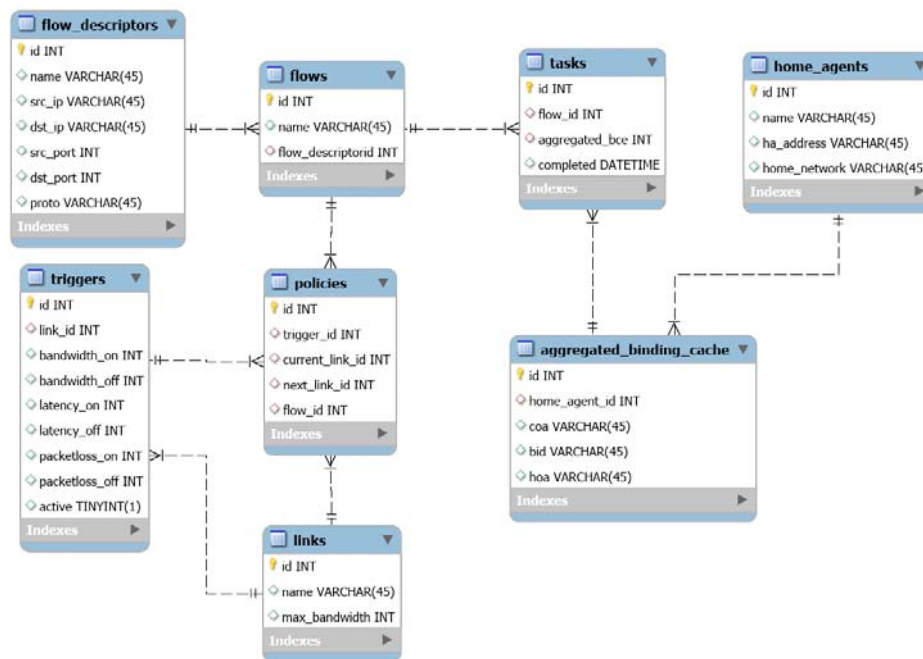


Figure 3-5: Policy Server database layout

3.2.1.3.1.1 flow_desciptor table

Used to identify a single flow based on 5-tuple information.

Field Name	Data type	Comment
id	integer	Unique key
name	string	Name of the stream
src_ip	IPv6 address	Source IPv6 address
dst_ip	IPv6 address	Destination IPv6 address
src_port	integer	Source TCP/UDP port
dst_port	integer	Destination TCP/UDP port
proto	integer	Transport protocol id.

3.2.1.3.1.2 flows table

As flow descriptors only identify a single flow, to identify a protocol consisting of several different flows, another abstraction layer is used.

Field Name	Data type	Comment
id	integer	Unique key
name	string	Protocol name
flow_descriptor_id	integer	Flow descriptor id key

3.2.1.3.1.3 home_agents table

This table stores administrative information for each Home Agent.

Field Name	Data type	Comment
id	integer	Unique key
name	string	Name of the Home Agent
ha_address	IPv6 address	Home Agent address
home_network	IPv6 prefix	Home Network

3.2.1.3.1.4 aggregated_binding_cache table

BCE entries received in the policyRequest messages are stored here.

Field Name	Data type	Comment
id	integer	Unique key
home_agent_id	integer	Home Agent id
hoa	IPv6 address	Home Address
coa	IPv6 address	Care-Of Address
bid	integer	Binding Identifier

3.2.1.3.1.5 tasks table

Policy decisions are stored here. New entries are sent to the HA with the policyCommand message. Acknowledgement sets the completed field.

Field Name	Data type	Comment
id	integer	Unique key
flow_id	integer	Protocol flow id
aggregated_bce_id	integer	Aggr. Binding Cache Entry id.

3.2.1.3.1.6 triggers table

Trigger statements are stored here.

Field Name	Data type	Comment
id	integer	Unique key
link_id	integer	Link id
bandwidth_on	integer	Policy valid if exceeded.
bandwidth_off	integer	Policy invalid if exceeded.
packetloss_on	integer	Policy valid if exceeded.
packetloss_off	integer	Policy invalid if exceeded.
delay_on	integer	Policy valid if exceeded.
delay_off	integer	Policy invalid if exceeded.
active	integer	Turn on/off trigger.

3.2.1.3.1.7 policies table

Applicable policies are stored in this table, filled by trigger. Moves flow from one link to another.

Field Name	Data type	Comment
id	integer	Unique key
trigger_id	integer	Trigger id.

current_link_id	integer	Current link id.
next_link_id	integer	Next link id.
flow_id	integer	Flow id.

3.2.1.3.1.8 links table

Stores link information.

Field Name	Data type	Comment
id	integer	Unique key
name	integer	Name (BID)
max_bandwidth	integer	Link capacity

3.2.1.3.2 *Threads*

3.2.1.3.3 *Measurement thread*

Listens for measurements and stores aggregated network statistics in the links table. The first version of the application does not store per-flow information, it aggregates network statistics and continuously updates the links table.

3.2.1.3.4 *PolicyRequest thread*

Listens for policyRequest messages and updates the aggregated_binding_cache table

3.2.1.3.5 *PolicyCommand thread*

Started by the decision module. Sends new tasks to the Home Agent, and waits for acknowledgement.

3.2.1.3.6 *Measurement Node*

In order to have a flexible and free solution to classify and account various flows on several network links we needed an open source software that builds top of the existing traffic management tools of the Linux operating system.

3.2.1.3.7 *Netfilter nfacct and ulogd framework*

Nfacct (*nfnetlink_acct*) is a new kernel module that appeared in the recent 3.3 version of the Linux kernel, which enables Netfilter with flexible accounting capabilities. The accounting framework is managed by the *nfacct* user space utility.

```
# nfacct help
nfacct v1.0.0: utility for the Netfilter extended accounting infrastructure
Usage: nfacct command [parameters]...

Commands:
  list [reset]          List the accounting object table (and reset)
  add object-name       Add new accounting object to table
  delete object-name    Delete existing accounting object
  get object-name       Get existing accounting object
  flush                Flush accounting object table
  version               Display version and disclaimer
  help                 Display this help message
```

The accounting object is a label which will contain statistical traffic data and it is added with the following command:

```
nfacct add http-ipv6
nfacct add https-ipv6
```

The label is used in *nfacct* match module as an identifier. For example, the following commands assign http and https IPv6 traffic to two separate accounting objects.

```
ip6tables -I INPUT -p tcp --sport 80 -m nfacct --nfacct-name http-ipv6
```

```

iptables -I INPUT -p tcp --sport 443 -m nfacct --nfacct-name https-ipv6

iptables -I OUTPUT -p tcp --dport 80 -m nfacct --nfacct-name http-ipv6

iptables -I OUTPUT -p tcp --dport 443 -m nfacct --nfacct-name https-ipv6

```

In order to gain real time data from the accounting subsystem another Netfilter module called *ulogd2* is required, which is a user space daemon configured to continuously deliver well-formatted data from the Netfilter subsystem based on its configuration.

An example of the XML output generated by the *ulogd2* utility, showing the data gathered from the *nfacct* subsystem:

```

<obj><name>http-
ipv6</name><pkts>0000000000000000009</pkts><bytes>0000000000000000408</
bytes><hour>11</hour><min>13</min><sec>55</sec><wday>5</wday><day>12</day><month>10</mon
th><year>2012</year></obj>

<obj><name>https-
ipv6</name><pkts>00000000000000000031</pkts><bytes>00000000000000004041</bytes><hour>11<
/hour><min>13</min><sec>55</sec><wday>5</wday><day>12</day><month>10</month><year>2012</
year></obj>

```

The *ulogd2* utility supports several output formats. The quickest way to send the statistics over the network is to log to the *stdout* and pipe the data to *netcat* which connects to the policy server.

3.2.1.3.8 Measurement node simulator

Unfortunately due to the complexity of the overall system, gathering and processing distributed network statistics was not possible given the short timeframe of the research, instead a fluctuating link usage was simulated on the Policy Server node which subsequently updated the various statistics fields in the links table.

3.2.1.3.9 Home Agent

The worker running on the HA has three main tasks: sending *policyReq* messages in which the HA synchronizes its Binding Cache with the Policy Server, maintaining flow bindings after receiving *policyCmd* messages and synchronizing the bindings with the Mobile Router.

The JSON¹ formatted data contains the HoA and the BID identifiers to select the egress interface of a given UE. It also contains a list of flow descriptors to be applied for a given UE on both MR and HA sides.

```
[{"hoa"=>["2001:738:1030:1:0:0:0:2"], "bid"=>"100", "proto"=>"any"}]
```

The command towards the Netfilter framework is compiled from the message and flow binding is set via the *iptables* utility using the following scheme:

¹ JavaScript Object Notation, <http://www.json.org/>

```
ip6tables -A PREROUTING -t mangle -p <proto> -s <source ip> -d <dest ip> --sport <source
port> --dport <dest port> -j MARK --set-mark <bid>
```

Once the rules are installed the policy routing is performed using the networking subsystem of the Linux kernel. The following figure describes the process:

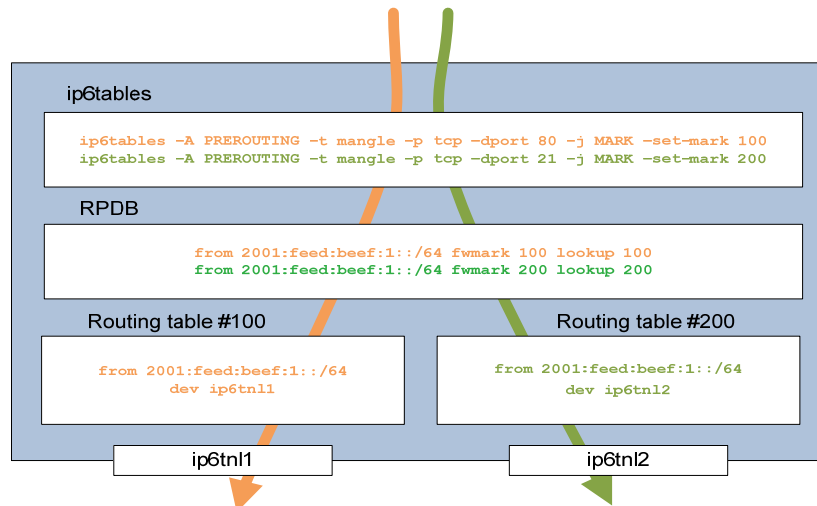


Figure 3-6: Data flow inside the Linux kernel

In order to speed up the implementation, the authors plan to implement interfacing with the *Netfilter* architecture using a library instead of running a system command.

A very important step in the policy exchange mechanism is the synchronization of flow bindings between the MN/MR and the HA. This is achieved based on the same *policyCmd* message, however the directionality of the bound data flow is different on the MN/MR and HA side. As a result of this behavior, data flows are represented from the Correspondent Node's point of view. This representation follows the convention set by the original Flow Bindings IETF standard (RFC 6089).

The communication between the MN/MR and HA is implemented using SSH RPC² calls. Integration with the IPv6 mobility daemon is planned for a future release. Using SSH RPC the stability of the signaling channel is ensured and the acknowledgement of the command is returned by the RPC as well.

3.2.1.3.9.1 Example Command on the Home Agent

```
ip6tables -A PREROUTING -t mangle -p <proto> -s <source ip> -d <dest ip> --sport <source
port> --dport <dest port> -j MARK --set-mark <bid>
```

3.2.1.3.9.2 Example RPC command to the Mobile Router

```
ssh <HoA> ip6tables -A PREROUTING -t mangle -p <proto> -s <source ip> -d <dest ip> --
sport <source port> --dport <dest port> -j MARK --set-mark <bid>
```

² Secure Shell Remote Procedure Call

3.2.1.4 Measurement results

Three main use cases were examined. Default Flow Binding Provisioning (1) is used for example in an environment where a central entity wants to force Service Level Agreements (SLA) to a customer, e.g., forcing P2P traffic through WiFi while allowing UMTS access for HTTP traffic. The Traffic Offloading use case (2) makes it possible to move certain data flows from one interface to another, e.g., in case of increasing traffic load in 3G segment move video streams to the Wi-Fi segment. Policies can be much complex based on the fact that the core network entities know about their actual traffic conditions. Flow Binding Revocation (3) is useful when due to an administrative decision a certain flow binding is no longer valid for the MN.

Different load-balancing techniques were implemented with respect to the above use-cases and the overall stability of the network.

For example, the Round-robin algorithm (flows are distributed among available uplinks evenly) requires no input arguments as it always produces the same behavior regardless of the actual network status. The actual per-hour user numbers are represented on the right y-axis, while actual throughput is depicted on the left y-axis. Each user spend exactly 1 hour in the network. If users would continue to use the network throughout the day, the distribution would be an incremental value and it would not demonstrate the properties of the algorithm. Figure 3-7 shows that the RR algorithm evenly distributes the incoming bursts and keeps the backhaul segments from reaching the maximum capacity and getting overloaded.

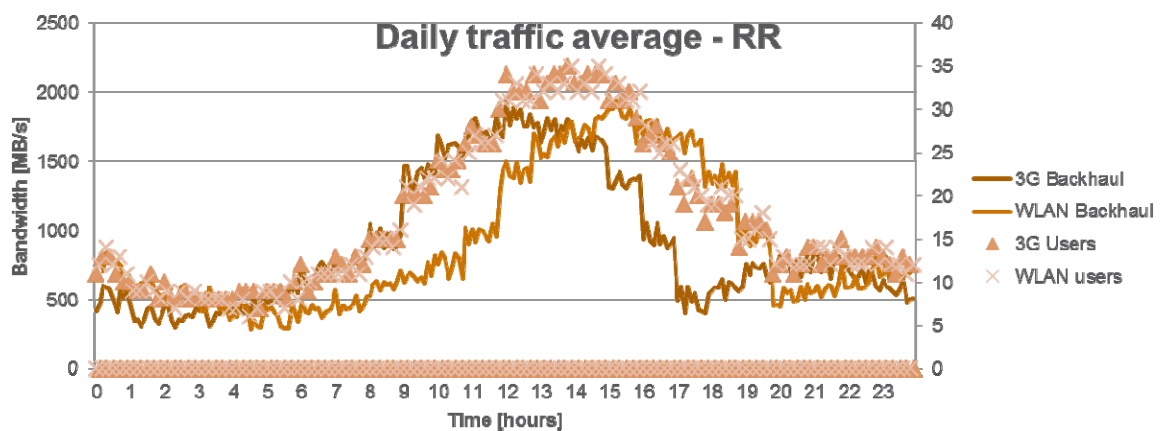


Figure 3-7: Performance of the Round-robin decision algorithm

The Figure 3-8 presents the state where the decision-making algorithm considers additional input parameters such as actual bandwidth, user count of the network. In this scenario the Least Used (implements dynamic selection based on the recently used link) and Overflow (waits until one of the links become full, allowing network policy events to be triggered before utilizing all available media) algorithms were applied, where the Least Used solution pushes new UE traffic to the backhaul link where the actual bandwidth is the least, and Overflow selects one backhaul and only diverts flows to a different backhaul when the resources of the current one are exhausted.

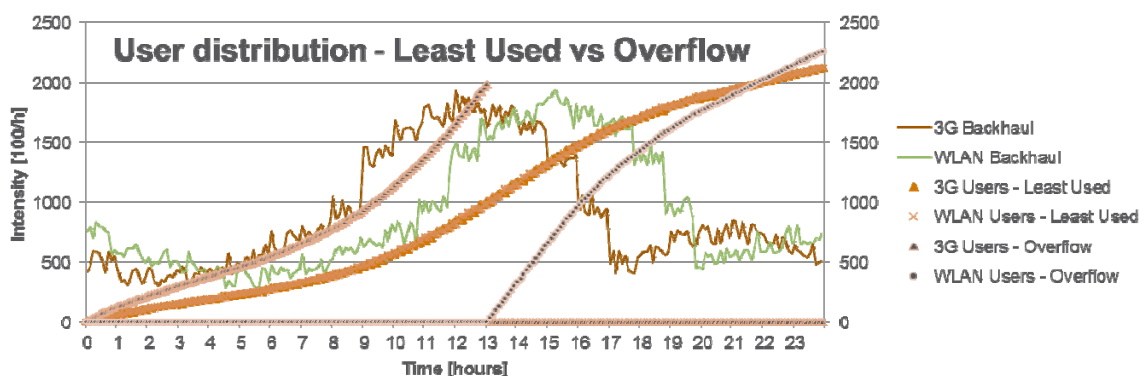


Figure 3-8: Performance of the Least used and Overflow algorithms

The following assumptions are valid in this scenario: each user stays connected to the network in order to have accumulating traffic, all users generate a traffic data-flow and previously used bandwidth distribution may be used as incoming intensity for the number of newly connected users per hour. One of the greatest advantages of the Least Used algorithm is when each user consumes the same amount of

bandwidth and the distribution is proportional to the incoming intensity; thereby the system stays stable throughout the analyzed timeframe. The Overflow algorithm, however, highly depends on the configuration of the system: when the handoff parameter of the algorithm is set to 100%, the system waits until one of the links reaches 100% load, and only after then it starts to relocate data flows. Therefore we conclude that the latter algorithm is suboptimal due to static input parameters. Further results and more details on the measurements based on our NB-IFOM testbed can be found in document D4.4.1.

3.2.1.5 Scalability

Not only the scalability of the architecture, but the scalability of the implementation is essential to handle carrier grade traffic and flow count. Therefore the following remarks serve as guidelines for future implementers of the technology.

The database, which stores the centralized flow information of every UE is the most critical component. Using modern Relational database management systems such as Oracle, MySQL, etc. the ability to horizontally or vertically scale the database backend over multiple nodes is available at hand, and it single handedly eliminates the problem of single point-of-failure and load-balancing.

The bottleneck of the actual and future implementations would be the Home Agent. Currently HA implementations are not ready to serve large quantities of UEs and they are quite unstable; hence the lack of large-scale performance tests of our solution is quite substantial. In order to eliminate the scalability a problem of the Home Agent, a new implementation is required which scales well with recent features of the kernel of the operating system. One of the promising solutions is the MIP6D-NG³ project which implements XFRM tunneling inside the Linux kernel, speeding up the internal processes of the mobility component. To overcome the single point-of-failure issue, Global HA to HA communication should be implemented which allow multiple Home Agent nodes to operate for the same UE domain.

3.2.2 QoE-aware Traffic Engineered Handovers

In a context of scarce resources, the demand of high and reliable QoE in nowadays applications stresses the need to optimize the EPC path w.r.t. QoS & QoE. One way to achieve this is the RAT change in order to balance the traffic or get a better QoS with the hope to improve the QoE. Where as QoS is achievable at the EPS level, there is a need to anticipate the QoE impact of an EPC path change at the e2e level. The key tools to drive traffic switching between 3GPP and non 3GPP technology are ANDSF, MIH and IP Mobility. However their view on a connection is restricted to the EPS scope. On the other hand, a transport topology aware application protocol to assist the selection of overlay application CNs, such as the IETF ALTO protocol, see [ALI11], has an e2e view on a connection, but no insight below the EPS level. QoE-aware Traffic Engineered HO (TEHO) solutions to harmonize both perspectives and scopes without decision conflicts have been proposed in D4.3.1, Section 3.4.3. The present section focuses on one of them, where ALTO is used after IP Mobility and helps readjusting the selection of application endpoints to connect to.

3.2.2.1 Basic idea of the proposed solutions

The prior art work on QoE aware Traffic Engineered HO (TEHO) has been exposed in D4.3.1, § 3.4.3.1. While the ANDSF, MIH or IP Mobility enable traffic offload and optimization of the network resources, their insight and decision scope however is limited to the LTE network: they cannot see the end to end path and thus take into account the QoE perceived at the UE, which is more and more challenged by massive use of resources and performance greedy applications. On the other hand, it is not the responsibility of the ALTO protocol to care about the UE mobility. Nevertheless, the mobility of a UE can impact its path to the PDN and thus the path to the resource location and thus the related QoE. Therefore, it is necessary to inform the UE, which can then take the appropriate decisions upon the changes occurred in its path. Currently, during mobility there is no association between network level information and application level information when a HO occurs.

The QoE aware TEHO scheme proposed here aims at jointly improve QoS and QoE in HO decisions by proactively or reactively associating QoE continuity to the HO decision. The scheme introduces the usage of selection mechanisms of correspondent nodes in overlay applications, triggered after of during an inter-RAT HO or upon a change in the S5/S8 bearer upon intra E-UTRAN HO. Three corresponding solutions are exposed in D4.3.1, Section 3.4.3. In this deliverable we focus on the usage of the ALTO protocol after IP Mobility, referred to as Adaptive QoE aware TEHO.

3.2.2.2 Solution : adaptive QoE aware TEHO

This solution consists in checking the end to end quality of the path between the UE and the candidate CNs, which are also the endpoints of applications that offer the choice of several endpoints to connect

³ <http://www.mip6d-ng.net/>

with, as it is the case for P2P or Contend Delivery. The checking is done by using the ALTO protocol that can provide Application Clients with the Endpoint (EP) Cost associated to the set of previously selected candidate Endpoints. If the cost has changed after IP Mobility and if, in particular, one of the candidate EPs offers a better cost than the one the UE is currently connected to, the UE can connect to this better EP getting thus additional QoE improvement to the one already gained through IP Mobility.

In this example, IP Mobility causes a change from SGW1 to SGW2 and subsequently a change of the associated path cost from UE to the EPs. Once a HO is performed the CM requests ALTO Client to update its path costs to the current CNs/EPs.

Suppose the cost of the e2e path from UE to EP is defined as $\text{MAX}[P(\text{EP}, \text{PGW}), P(\text{PGW}, \text{UE})]$, and is to be minimized. In this example the path cost from UE to PGW evolves from 7.5 to 5. With SGW2, the least cost EP becomes EP2 with $C=5$, where as the cost with EP1 equals 7.5; therefore EP2 is preferable. Note that a cost model of type $C = \text{MAX}_i(C_i)$ is frequent when the worst value must be taken over the C_i , for instance to evaluate the cost in terms of bandwidth availability.

On the IP route between UE and PGW lies the Serving Gateway (SGW) to which the UE is attached. Suppose that IP Mobility causes a change of SGW: the path between the serving EP and the UE is thus changed, in its last hop, between the PGW and the SGW.

Although, after IP Mobility, the list of candidate EPs remains the same, the associated downloading and routing cost may have changed and needs to be updated. A possible consequence is that the EP currently used to download from is no more optimal and needs to be changed.

The UE is notified by the connection manager (CM) of the change in the EPC path in order to re-evaluate the cost of relevant EPs. The CM is also aware of the IP flows sent or received by the UE. When a change in the IP flow routing policies is detected, the CM triggers the ALTO client who can subsequently request an update of the costs to the eligible EPs, as illustrated on Figure 3-9. Upon reception of the new cost values, the ALTO client could decide to change its corresponding EP. The UE may implement the specifications described in <http://tools.ietf.org/id/draft-ietf-netext-logical-interface-support-02.txt>.

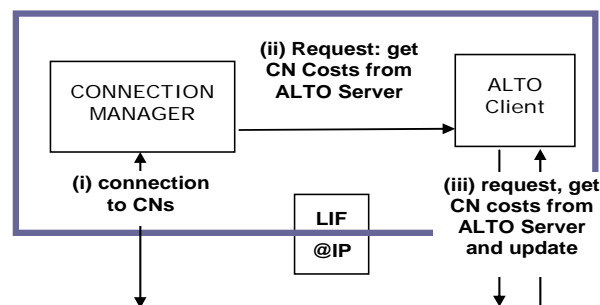


Figure 3-9: ALTO assisted connection management in Evolved Packet Systems (ALTO-COMEPS): architecture on an IFOM capable UE

• IP Mobility-capable UE

- IP Mobility causes change from SGW1 to SGW2 subsequently a change of the associated path cost from UE to the EPs.
- CM then requests ALTO Client to update its path costs to the current CNs/EPs
- Suppose cost of e2e path from UE to EP is defined as $\text{MAX}[P(\text{EP}, \text{PGW}), P(\text{PGW}, \text{UE})]$ and to be minimized.
- In this example, path cost from UE to EP evolves from 7.5 to 5. With SGW2, the least cost EP becomes EP2 with $C=5$, whereas the cost with EP1 equals 7.5, so EP2 is preferable.

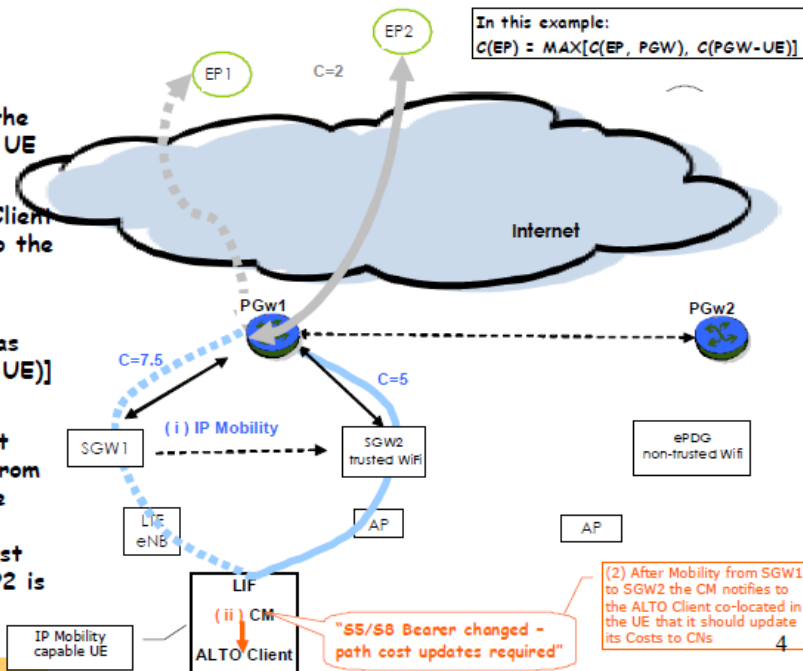


Figure 3-10: ALTO used upon IP mobility to update path costs between UEs and Endpoints and triggering connection to a better candidate application Endpoint (EP2)

3.2.2.3 Achievements

- A proof of concept has been demonstrated for the association of the ALTO protocol and IP mobility. This demonstration involves the base ALTO protocol and its scenario is shown in Figure 3-11.

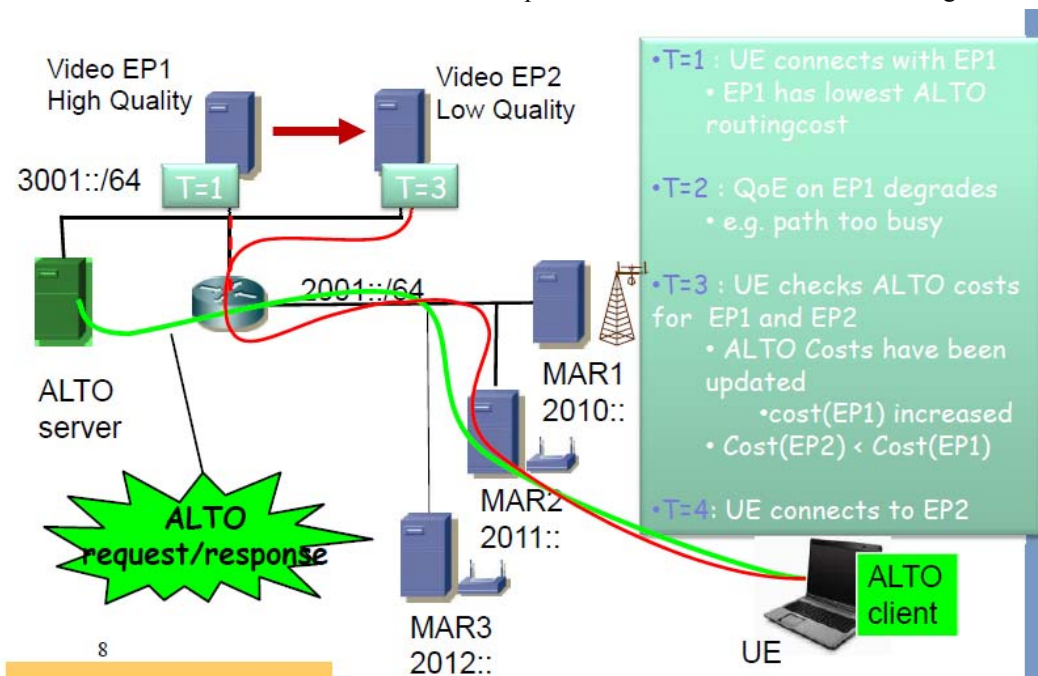


Figure 3-11: Scenario for the proof of concept shown to demonstrate the cooperation of the ALTO protocol with IP mobility

- Together with this proof of concept and ALTO protocol extension called ALTO Cost Schedule, has been proposed and presented at the IETF, see [Randriamasy12] and [Randriamasy12-2]. The principle and utility of this extension is described in Section 5.2.1. The set up of the demonstrated proof of concept is further described in D4.4.1.

3.2.3 Support of multipath flows

TCP is the prevalent reliable transport layer protocol used in the Internet to carry user data. Usually, a single path between the TCP sender and receiver is used to carry TCP traffic. In that case, TCP throughput is limited to the capacity of the bottleneck link on the path. Instead, if multiple paths are used simultaneously to aggregate the bandwidth the TCP performance may increase. It has been already shown that the potential of the multipath solution lies not only in providing robustness but also, in conjunction with an appropriate congestion controller, in providing means to balance the Internet congestion in a stable way. Despite these benefits, several issues concerning multipath transport of TCP still remain to be addressed before it can be successfully deployed. These include (i) reducing the impact of out-of-order delivery, and (ii) relaxing the requirement of support from the end-hosts.

3.2.3.1 Out-of-Order Packet Receptions

Since multiple paths may have different delays, higher-sequence-numbered packets scheduled for shorter delay paths may arrive at the receiver before the lower-sequence-numbered packets scheduled to the paths with longer delays.

TCP performance suffers from out-of-order packets mainly because of duplicate acknowledgement (DUPACK) generation. When TCP receiver gets an out-of-order packet, it generates a DUPACK. Reception of three DUPACKs cause TCP sender to unnecessarily trigger the fast retransmission/recovery algorithms.

Out-of-order packet receptions problem for TCP over multiple paths is illustrated in Figure 3-12. At time θ , TCP data packets are scheduled to two paths with different delays in round robin (RR) (Figure 3-12a). Path 1 has a delay of T and Path 2 has a delay of $2T$. TCP data packets (D1...6) are scheduled to these two paths in RR fashion: packets with odd sequence numbers are scheduled to the long path and packets with even sequence numbers are scheduled to the short path.

Figure 3-12b shows the situation after time T : packets scheduled for Path 1 arrive at the TCP receiver. TCP receiver buffers packets that arrived. Since TCP receiver expects D1 to arrive, it generates a DUPACK (i.e., an ACK with cumulative ACK sequence number 1 (i.e., A1)) for each out-of-order packet arrival. When TCP sender gets these 3 DUPACKs, it assumes that segment D1 is lost and triggers fast retransmit/recovery.

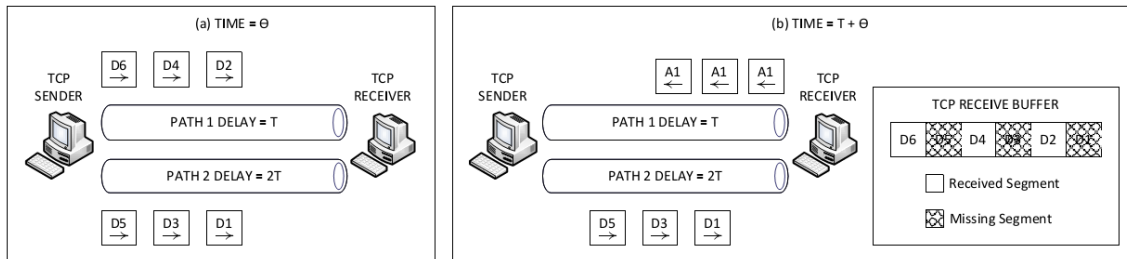


Figure 3-12: Out-of-Order Packets and TCP

A survey on the proposed solutions for out-of-order packet receptions when multiple paths are used is given in [Ayar12a].

3.2.3.2 Deployment and Adoption

We may divide current TCP over multiple paths proposals into 3 classes from deployment point of view: (1) End host based, (2) Proxy-aided, and (3) Proxy-based proposals:

1. *End-host based* solutions have components only on the TCP end-points. TCP sender and/or receiver TCP/IP stack implementation is modified to handle multiple-path related issues.
2. In addition to end-host changes, *proxy-aided* solutions have some components on a network element (i.e., a proxy) in-between the TCP sender and receiver. The proxy helps in handling the multiple-path related issues by supplying feedback to TCP sender/receiver.
3. *Proxy-based* solutions work completely transparent to TCP sender and receiver. Proxy detects TCP connections, splits TCP packets to multiple paths, and shapes TCP traffic so that TCP sender and receiver are not aware of the fact that multiple paths are used to carry TCP traffic in between.

End-host based and Proxy-aided solutions have a low chance of deployment and adoption since they require changes on the end-host TCP/IP protocol stacks. Thus, we concentrate on the proxy-based solutions [Ayar12b] in the MEVICO project.

3.2.3.3 Splitter/Combiner Architecture (SCA) and SCA Proxies (SCAPs)

We proposed SCA in [Ayar12b] which enables proxy-based TCP over multiple-paths solutions. SCA introduces a thin layer that is located above the forwarding layer which supplies multiple paths functionality (e.g., via multi-path routing, IP-in-IP encapsulation or tunneling, etc.). SCA uses TCP headers of passing packets to observe TCP connections and shapes TCP data/ACK traffic to increase goodput of TCP sender. SCA has following components (Figure 3-13):

- Packet Classifier classifies the TCP packets according to the header information and passes them to a related component.
- Connection Handler manages TCP connection records. TCP connection establishment/release packets (i.e., packets with SYN, RST, or FIN flags set) are used to create and delete records for TCP connections.
- Multiple Pipes Adapter interacts with the forwarding layer to access and use available multiple paths. In order to shield how multiple paths are used, we use the term pipe instead of path. Other SCA components use the Multiple Pipes Adapter APIs to get information about the pipes that may be used and to send data via them.
- Data/ACK Processor is responsible for handling data/ACK packets. Data/ACK packets may be delayed, dropped, or duplicated so that multiple path usage is shielded from the TCP end-points.
- Signaling Unit is responsible for signaling between SCA Proxies(SCAPs) on different network devices. Signaling information is used to probe for other SCAPs on the path between TCP sender and receiver, signaling information about lost packets, ...etc.
- Configuration and Management Unit is used to set parameters for the SCA components.

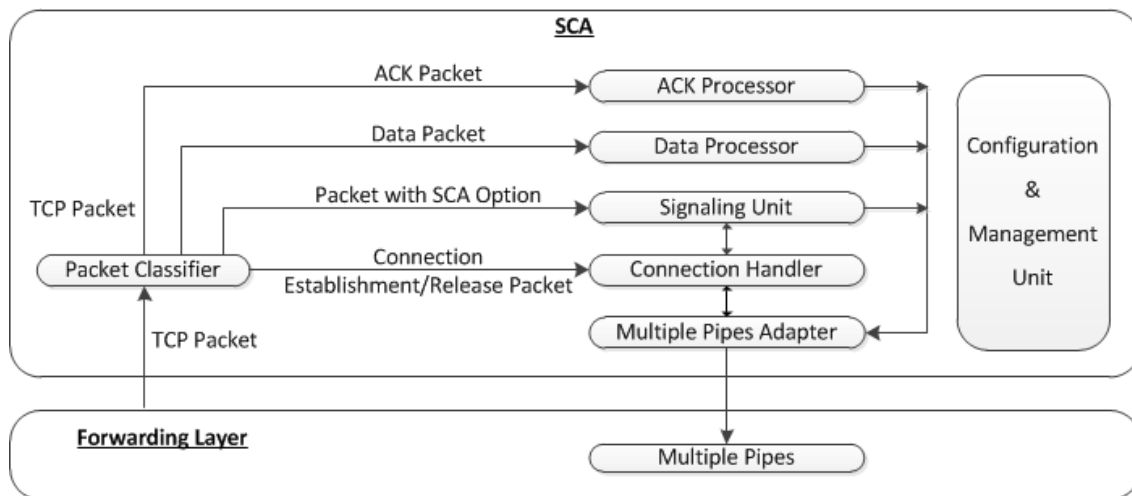


Figure 3-13: SCA Components

3.2.3.4 DUPACK Estimation and Filtering (DEF) Algorithm

DEF is a sample SCA application which works transparent to TCP end-points and eliminates out-of-order packets problem mentioned in Section 3.2.3.1. DEF uses RR scheduling of packets to paths. DUPACKs may be generated as a result of scheduling packets to different delay paths or real packet losses. DEF works by differentiating scheduling-based DUPACKs and loss-based DUPACKs. That is, DEF filters scheduling-based DUPACKs and passes loss-based DUPACKs.

As shown in Figure 3-14 [Ayar12c], DEF will be either in NO_LOSS state or in RETRANSMISSION state:

1. **NO_LOSS State:** When data transmission of a connection is started, DEF enters NO_LOSS state. DEF uses all the available pipes in round-robin (RR) for packet transmission till a retransmission is observed. In order to detect retransmissions, DEF tests, if the sequence number

of the current received packet is smaller than the highest sequence number ever received. If this is true RETRANSMISSION state is entered.

- DUPACKs are harmful if TCP sender is in the NO_LOSS state (i.e., either in slow-start or congestion avoidance phase) with increasing sequence numbers. Thus, DUPACK estimation and filtering algorithm is enabled in this state.
 - DUPACK estimator works in DEF data processor as follows: when a packet is scheduled for a pipe, its arrival time is estimated by adding its sending time to the RTT of the pipe. If there exists a segment with lower sequence number that had been scheduled before and whose expected arrival time is greater, a DUPACK must be generated by the receiver. Thus, an estimated_dupacks counter is incremented by 1.
 - DEF ACK processor keeps track of highest ACK number received so far for the connection. It uses this value to check whether a received ACK is a DUPACK or not. If a DUPACK is received, then the estimated_dupacks counter is checked. If it is non-zero, then the ACK is an expected RTT-difference-based DUPACK. DEF ACK processor simply filters (i.e., drops) the DUPACK and decrements the estimated_dupacks counter by 1. In that way, the TCP sender is prevented from reception of unnecessary DUPACKs.
2. RETRANSMISSION State: All the packets are scheduled to the shortest path in RETRANSMISSION state to minimize further RTT-difference based DUPACK generations.
- When TCP sender is in the RETRANSMISSION state (i.e., in fast retransmit/recovery), DUPACKs are useful since they provide the information about the number of in-flight packets and may give an opportunity to increase the TCP congestion window (cwnd). Thus, in this state, DEF algorithm is disabled.
 - DEF leaves RETRANSMISSION state and enters into NO_LOSS state if following conditions are satisfied:
 - i. New ACKs are received: TCP sender recovery phase may not be completed if there are still DUPACKs.
 - ii. All the data packets scheduled for the paths before entering the RETRANSMISSION state arrived to the receiver: so that packets scheduled for longer paths before entering the RETRANSMISSION state don't generate unexpected DUPACKs. Thus, DEF stays in RETRANSMISSION state at least for a duration of longest path's RTT.

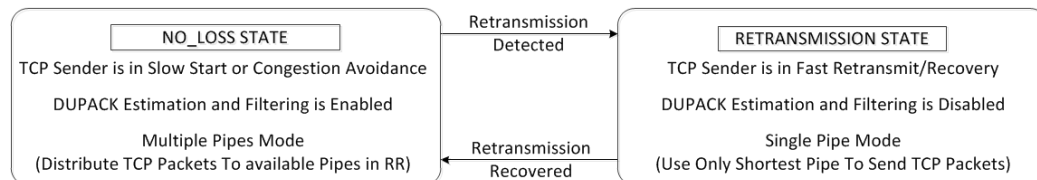


Figure 3-14: DEF States

3.3 Multi-Criteria cell selection

The growth and development in wireless network technologies requires drastic changes in wireless communication systems. Main reason of this big evolution is the increasing demands in mobile traffic which means increasing signal activity and traffic load in wireless systems with a limited spectrum. In order to meet these demands and provide the necessary capacities to support high data rate services, new wireless system architectures and models are investigated and standardized by 3rd generation partnership project (3GPP) [3GPP_TS_25.304], specifically through Long Term Evaluation (LTE) Release-8. Further studies are summarized in a technical report for initiating LTE-Advanced (LTE-A) standardization that defines the radio interface techniques [3GPP_TR_36.814]. LTE-A is standardized in [3GPP_TR_36.913] to increase the system throughput. Also heterogeneous network deployment is discussed and extensive scenarios are given besides the hierarchical macrocell deployment network scenarios.

In heterogeneous networks, different size of terminals with different cell layers, such as femto, pico, and relay nodes are placed in a random manner throughout a macrocell layout. Furthermore numerous access technologies can coexist in the heterogeneous networks, such as 3G cellular systems, WiFi and Bluetooth. Possessing these features, heterogeneous networks have some challenges that should be handled by

adaptive methods due to complexity of the system. An illustration of heterogeneous networks can be seen in Figure 3-15.

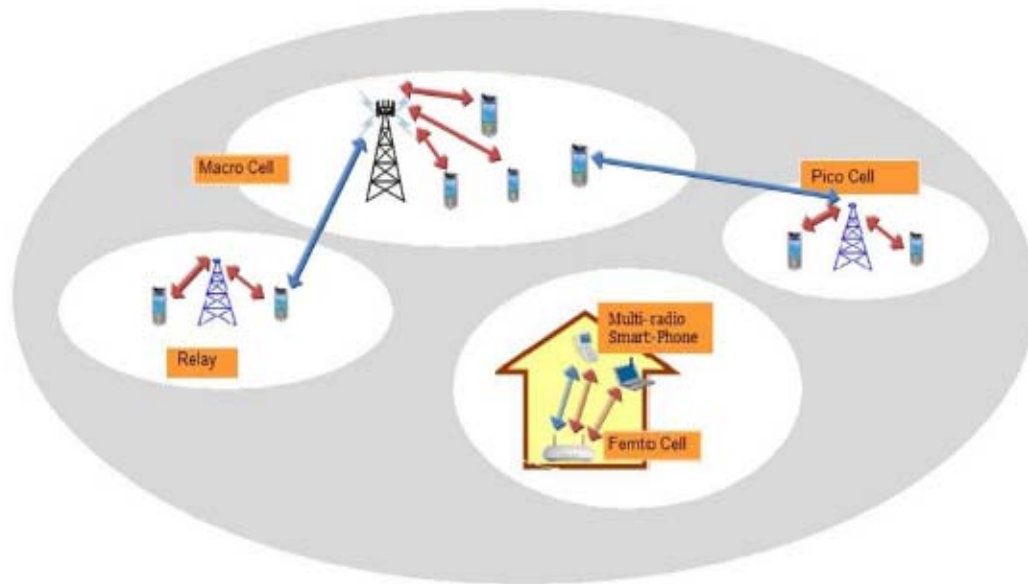


Figure 3-15: Heterogeneous Networks

In heterogeneous networks, different size of terminals with different cell layers, such as femto, pico, and relay nodes are placed in a random manner throughout a macrocell layout. Furthermore numerous access technologies can coexist in the heterogeneous networks, such as 3G cellular systems, WiFi and Bluetooth. Possessing these features, heterogeneous networks have some challenges that should be handled by adaptive methods due to complexity of the system. An illustration of heterogeneous networks can be seen in Figure 1. One complex issue is the cross tier interference that is derived from one cell to other cells causing significant degradation in the communication. Another important issue is the handover caused by seamless transition from one network to another, such as switching between cells of the users. Many metrics such as signal strength, distance, signal- to-noise ratio (SNR), bit error rate (BER), traffic load, quality indicator and some combination of these indicators can be used in order to decide if the handover is required or not. Therefore, it requires intelligent mechanisms for mobility management. Decreasing the number of handover can be achieved by utilizing proper cell selection techniques. Cell selection is a determination process that helps to provide a sufficient service to each mobile station from a suitable cell in order to maintain the required quality of service (QoS) for each BS and to balance the system load.

Since there are many ways to build a heterogeneous network, some important points must be considered while planning the deployment of nodes, such as picocells, macrocells or femtocells, in the network. The answers of where and how many nodes should be deployed play an important role in increasing the system throughput. Even there are small nodes in high traffic zones; most users in the network continue to receive the strongest signal from the macrocell BSs. Therefore users are still connected to the macrocell BS. In order to make a fairer cell association, mobile users can be shifted to the lightly loaded BSs by different strategies. In case of the existence of femtocells in heterogeneous networks, there are some other parameters that should be considered in the cell selection process. One of them is the access mode of the femtocells [Simsek11]. There are three different access modes in femtocells which are closed mode, open mode and hybrid mode [Perez09]. In closed access mode, a set of registered user equipments (UEs) belonging to close access femtocells are allowed to access a femtocell. This type of femtocell access control strategy can be applied in residential deployment scenarios. However, in public places such as airports and shopping malls, open access mode of femtocells can also be used where any UE can access the femtocell and benefit from its services. This access mode is usually used to improve indoor coverage. In hybrid access mode, any UE may access the femtocell but preference would be given to those UEs which subscribe to the femtocell. According to these access methods, different cell selection methods are studied in order to obtain the best performance provided by the upper bound access mode, in which each UE can select either macro cell or femtocell. The best performance is observed in open access mode case in femtocells. In LTE and LTE-A systems one of the cell selection method is the Reference Signal Received Power based cell selection (RSRP-based cell selection) which compares the downlink signal transmitted from neighboring cells and the largest selected RSRP as the serving cell by mobile users. Another method for cell selection is Reference Signal Received Quality (RSRQ based cell selection) which provides additional information when RSRP is not sufficient to make a reliable handover or cell reselection decision. RSRQ is the ratio between the RSRP and the Received Signal Strength Indicator

(RSSI), and depending on the measurement bandwidth, means the number of resource blocks [2]. In addition to these standardized methods, a new technique called signal to interference plus noise power ratio (SINR)-based cell selection is investigated in order to consider the intercell interference coordination effect since it is very important to improve the system and cell edge throughput [Sangiamwong11]. Achieving a balanced user association to the cells will reduce the load on the macrocell, so that better service can be maintained to its remaining users. Load balancing is a very recent research topic for heterogeneous networks. The reason is that these networks are more sensitive to the cell selection and user association policy than traditional load balancing schemes where they are applied to macrocell-only networks. In the study of [Okino11], authors present an offloading method by using a cell range expansion (CRE) algorithm for load balancing. The CRE approach is an effective method to balance the load in the heterogeneous network. It is also known as cell biasing technique in the literature. The cell selection process is realized by biasing the measured signal that balances the load among the BSs. However this approach causes significant interference for the picocell edge users by the macrocell BS. Therefore, how to design the biasing factor and mitigate the interference are important open problem. Authors investigate various biasing factors considering the downlink interference in LTE-A system. Another recent study in load balancing is presented in [Rong12] by considering jointly the resource allocation scheme with the cell association algorithm.

3.3.1 Multi-criteria Cell Selection Algorithms

We consider an LTE-based heterogeneous network consisting of macrocells, picocells and femtocells. In such a network traditional cell association methods, such as SINR based cell selection, result with a very unbalanced deployment of the users. For instance most of the users are associated with the macrocell since they receive higher SINR values than the other small cells. In order to obtain fairer deployment among all the tiers, the received rate metric should be utilized in cell selection approaches. Although this metric is a function of SINR, over loaded cells have lower overall long term rate. This decreases the system throughput. Main objective of the small cells is to increase the network performance by offloading from the macrocells. It is important to maximize both the sum rate and the user rate.

The achievable user rate of the user k from BS i is calculated as follows:

$$R_{ij} = \log_2 (1 + \gamma_{ij})$$

where γ_{ij} is the SINR value of the j^{th} user received from the i^{th} BS and it is calculated as follows:

$$\gamma_{j,i} = \frac{P_i |\bar{h}_{j,i}|^2}{N_0 + I_j}; \quad i = 1, \dots, U$$

where P_i is the transmit power of BS i , $\bar{h}_{j,i}$ denotes the average channel coefficient between the user j and BS i that includes pathloss, shadowing and multipath effect, U denotes the total number of the cells, N_0 is the Additive White Gaussian Noise (AWGN) and $I_j = \sum_{u=1; u \neq i}^U |h_{j,u}|^2$ is the total amount of interference which is caused by other cells.

3.3.1.1 SINR Based Cell Selection Algorithm

SINR-based cell selection is achieved by the following criteria:

$$i_{\text{SINR}} = \arg \max_i \gamma_{j,i}$$

where i_{SINR} is the selected cell index based on the SINR-based criteria.

3.3.1.2 Distance Based Cell Selection Algorithm:

In this approach, the users are associated with the nearest BS in the network. It can be mathematically expressed as follows:

$$i_{\text{Distance}} = \arg \min_i d_{j,i}$$

where i_{Distance} is the selected cell index based on the Distance-Based criteria and $d_{j,i}$ is the distance value from the i^{th} cell to the mobile user j .

3.3.1.3 Biased SINR Based Cell Selection Algorithm:

In this approach, the users are connected to the BS with the highest biased SINR [Rong12]. This method is also known as cell range expansion (CRE) technique. This approach can be expressed as follows:

$$i_{\text{BSINR}} = \arg \min_i (\beta_i \gamma_{j,i})$$

where i_{BSINR} is the selected cell index based on the biased SINR based criteria and where β_i denotes the biasing factor for the BS i .

This method enables the users to choose smaller cells with lower transmit power. It expands the range of small cells so that their coverage is extended. Therefore more users can connect to those cells; hence the load balancing is achieved among all the cells in the network.

3.3.1.4 The proposed cell selection algorithm

We propose a multicriteria cell selection algorithm which takes into account the user quality of service requirements, the load on the BSs and the achievable average rate. The proposed criterion is as follows:

$$i_{\text{Load}} = \arg \max_i r_{j,i}$$

where i_{Load} is the selected cell index based on the proposed criterion, and $r_{j,i}$ is the weighted rate coefficient for the user j from the i^{th} cell.

The weighted rate coefficient $r_{j,i}$ can be calculated as follows:

$$r_{j,i} = \frac{w_j \times R_{j,i}}{W_i + w_j}$$

where w_j is the rate requirements of user j , W_i is the total load of BS i and $R_{j,i}$ is the average supportable rate for user j by cell i .

The load of BS can be calculated by using different ways. The simplest method is to sum the user's data rate requirements that are previously assigned to BS i as:

$$W_i = \sum_{k=1}^K w_k, \quad k = 1, 2, \dots, K$$

where K denotes the total number of the users that are assigned to BS i .

3.3.2 Summary of Evaluation Results

The MCCS algorithms mentioned above are evaluated based on the average user throughput and utilization of different cell sites.

The results on the CDF of user throughput show that Traffic Load Based method (the proposed method) performs the best. The results of the Biased SINR Based method are close to the Traffic Load Based method.

The results on the utilization of cells also show that the load distribution is performed the best when the proposed method is used.

4 Microscopic traffic management

4.1 QoS differentiation based on applications and user profiles

4.1.1 Application and user classification

The new advanced radio technologies providing real mobile broadband packet data services comparable to the fixed internet, the penetration of smart phones combined together with the flat rate pricing used by the operators, continue contributing to the tremendous growth of the mobile data traffic. There are many reasons behind the need for application classification techniques: These reasons make application classification essential in traffic management in order to prioritize different application traffic in the network.

Application classification aims at understanding the internet usage better and grouping the various usage according to a “similarity” concept together. Defining the “similarity” is necessary so that classes can be formed, but this is not very straightforward most of the times. Our approach at this point was to classify the applications according to their QoS requirements, average amount of bit rates required, the effect of delay and jitter on the application are the main criteria on this.

In order to classify a usage over the internet, the usage needs to be identified, at least to an extent to provide the right QoS.

There are different techniques for application classification: (1) payload based classification that is based on the inspection of the packet content including or not the packet payload, and, (2) statistical based classification that consists on analysing the behavioural and statistical characteristics of the traffic (jitter, session time, inter-arrival, UL/DL distribution, packet size, etc.). Montimage and Ericsson Turkey work on the application classification problem. Montimage is working on their technique based on inspection of the contents of packets, whereas Ericsson Turkey is working on a method which can classify applications into categories Video, VoIP, Instant Messaging, P2P, Web Browsing, File Transfer and Gaming without necessarily knowing which particular application was utilized. Montimage is also supporting Ericsson in this effort.

4.1.1.1 Application Identification/Classification Mechanism

Montimage’s application classification technique is mainly based on the inspection of the contents of the packets. The inspection is performed by comparing the packet headers and application data to already defined signatures that identify different applications. The signatures which are used describe patterns that identify the nature of applications. It is clear that the accuracy of this method depends on the non-overlapping of the signatures. This property is not always easy to satisfy because of some similarities between the applications. Therefore, in addition to the pattern analysis, we add another layer for state analysis that consists on exploiting the sequence of steps of a protocol when it can be modelled using a state machine (example: an HTTP GET request will be followed by a valid HTTP response).

4.1.1.2 Application Identification initial results

The evaluation results presented in the following are based on sample trace files collected by Ericsson Turkey. The objective of the evaluation was mainly to build a ground truth base for the Bulk Traffic Analysis. Moreover, it provided a number of indicators in order to estimate the accuracy and cost of the classification mechanism. The traffic trace files were collected on PC machines connected to the fixed Internet by running the applications of interests (set of P2P applications, Web video, Skype) and recording the traffic activity.

Table 4.1 presents an overview of the application classification results performed on Ericsson’s trace files. The results show that the classification accuracy is relatively high reaching around 96% of the traffic data in terms of volume and number of packets. However, the accuracy in terms of number of flows is lower (82%). This result was expected as the trace files were captured on a local network, where the broadcast signalling (using UDP) is relatively high. Only 0.74% of TCP flows were left unclassified. Among the unclassified flows (TCP and UDP flows) only 5% has more than 10 packets. Table 4.2 provides the distribution of unclassified flows based on the number of packets. It shows that the majority of these flows contain few packets. While analysing the unclassified flows, we noticed that some of them were already initiated when the network sniffing was started. These cold start flows account for 62% of the data volume of unclassified flows though their number accounts for only 0.34% of the total flows number.

Table 4.1: Overview of the application classification results

	Flows Number	Packets Count	Bytes Count
TOTAL	30513	2733347	1916196927
Total Classified	25081	2622685	1839604663
Total Classified (%)	82.2%	95.95%	96.00%
Total Unkown	227	99657	75449273
Total Unkown (%)	0.74%	3.64%	3.93%
Total Unclassified (Unkown + UDP)	5432	110662	76592264
Total Unclassified (%) (Unkown + UDP)	17.8%	4.04%	3.99%

Table 4.2: Distribution of unclassified flows based on the number of packets

Packets Distribution	Flows Number	Bytes Count	Flows Number (Cold Start)	Bytes Count (Cold Start)
2 <= Packets	4751	0.67 MB	0	0
[3 : 10] Packets	423	0.34 MB	0	0
[11 : 100] Packets	213	0.92 MB	2	5.2 KB
100 + Packets	60	235.2 MB	17	147.7 MB
	5447	237.15 MB	19 (0.34 %)	147.7 MB (62.25 %)

Table 4.3: Sample of classified applications

Application Name	Flows Number	Packets Count	Bytes Count
Bittorrent	15459	1371049	1198970278
Skype	1370	617276	251476274
https	301	376751	181093125
http	4646	103548	82374039
Youtube	44	83611	79238629
Unknown	227	99657	75449273
Gnutella	206	16073	12545929
Dailymotion	20	11429	10789797
udp	5205	11005	1142991
Facebook	16	306	171212
Twitter	15	178	74266

As the number of Internet protocols and applications is high, the objective of the classification was not to identify each individual protocol/application; rather, we analyzed the popularity of the protocols/applications, identified the top ranked ones and included them in the classification engine. This explains the difference between the classification of WEB sites/applications like Facebook or Twitter and sites of lower popularity that were identified as HTTP traffic (see Table 4.3).

4.1.1.3 Application classification in the network architecture

Application classification of the network traffic can be used for different objectives.

- Understand the application mix and the usage trends: This can be done by periodically (weekly or monthly basis) recording traffic samples on the interface between the core network and the

operator's PDN. The traffic application classification in this case can be performed offline. The objective here is to support the operator with up-to-dated view about the network utilization.

- Policy control and enforcement: requires application classification in order to grant priority levels (based on QoS requirements for instance) to specific applications. In this case, there is a need for live application classification with high performance constraints with respect to the speed and latency (wire speed, low latency). The application classification engine can be integrated, in this case, integrated into the P-GW or installed on a dedicated probe to inspect the S5/S8 or SGi interfaces.

4.1.1.3.1 Bulk Analysis of Network Data and Classification

Deep Packet Inspection tools in network operators investigate the payload and can determine the exact application type such as Skype, Youtube, Dailymotion, Google+, etc. Please see *Hiba! A hivatkozási forrás nem található.* This may be required due to many reasons such as the operator's pricing strategy, campaigns or regulations. That is, these tools are mainly utilized for policy enforcement in real-time. However trying to map all the network traffic via real-time DPI would be extremely costly and many times unnecessary.

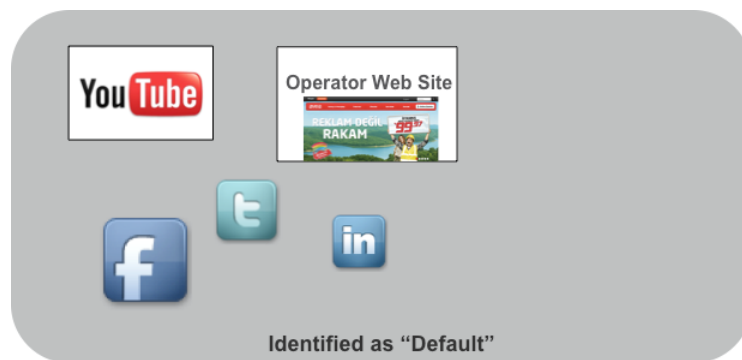


Figure 4-1: Illustration of how DPI classifies network traffic

For example, in case there is no specific restriction required, or any pricing strategy, there is no reason to identify whether a VoIP application is Skype or Google talk, however in order to satisfy QoS/QoE requirements and manage network efficiently, determining the family of application – that the application is VoIP- is very beneficial..

Ericsson Turkey has worked on a statistical method of classification This method aims to draw a map of the network traffic, that is, to classify the total usage according to varying time into several classes. The initial idea of classes were:

- Videostreaming
- VoIP
- Instant Messaging
- P2P filesharing
- Web surfing
- Gaming, and
- M2M

This has been modified and finalized as:

- Video streaming
- P2P
- Conversational (contains IM, VoIP and video chat)
- Web
- Gaming, and
- M2M

The main reason for grouping IM, VoIP and Video Chat in one class as conversational is that, the success of the statistical method in distinguishing the three was not acceptable. Merging these can be acceptable since the amount of packet flow is not as much as Video streaming and these three are similar in requirements and sufficiently different from the other classes.

This idea of mapping is illustrated in **Hiba! A hivatkozási forrás nem található.**



Figure 4-2: Bulk data analysis aims to bring out the distributions of applications in the MNO.

The initial aim is to get a mirror copy of data traffic going over the network for a period of time like one hour in a set pattern such as:

- Weekday work hour
- Weekday after work hour
- Weekday night
- Weekend daytime
- Weekend evening
- Weekend night

and get a map of the network as in **Hiba! A hivatkozási forrás nem található.** In case there are enough many such intervals, variation of usage during the week can be observed and the distribution of traffic into different applications can be observed.

This can be utilized to set QoS parameters according to distribution and the prioritization of the network operator. A very important concern which can be addressed by such a statistical solution is the subscriber privacy in the network. The amount of information gathered about usage's would not disturb the end users.

Another aim could be to classify users according to the applications and times they utilize the network and make proper campaigns to customers in order to make better use of the limited bandwidth.

In case this method can be improved so that it can run in real-time, it can be run on the flows where dpi is not running on and help network utilization in real-time and more importantly it may help network neutrality as well. The current progress does not allow real-time usage.

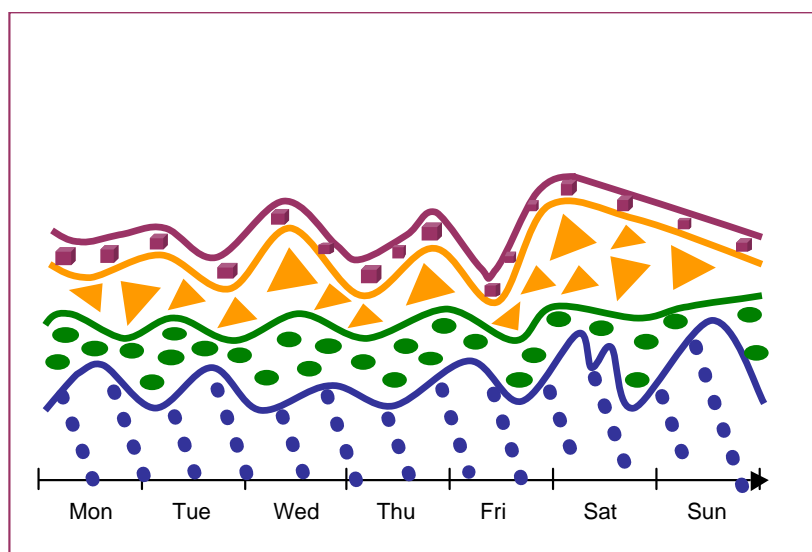


Figure 4-3: Weekly distribution of network data traffic into applications.

4.1.1.3.2 Bulk Analysis and Classification: Algorithm and Results

The work conducted during the statistical tool was basically working on a method to classify the flows from basic packet statistics. The particular features used were the packet size and packet direction.

We were challenged by the need to get a proper training set. We had some sampled traffic and we added some more samples so that as many kinds of applications as possible were generated.

After gathering the captures, we had to select individual flows and label them. In order to label the flows we needed to pass the flows through a DPI tool. Montimage volunteered for running through their DPI tool and providing the results in a format we requested.

Labeling the flows:

Even though each capture was produced to sample a specific usage of a specific application, it contained a variety of flows from background applications. Other than that even each youtube flow is not video, there is a lot of browsing in youtube usage.

Video Labeling: Since the aim of the application is to get the intrinsic characteristics of video, flows generated by browsing youtube should not be labeled as video. Only the specific flows carrying the video streams should be labeled as video. For this the content output of the DPI was checked. In case the content is mp4 or another video format detected by Montimage DPI, these flows were marked as video.

P2P Labeling: For P2P labeling, all the flows detected as P2P by the DPI were labeled as P2P.

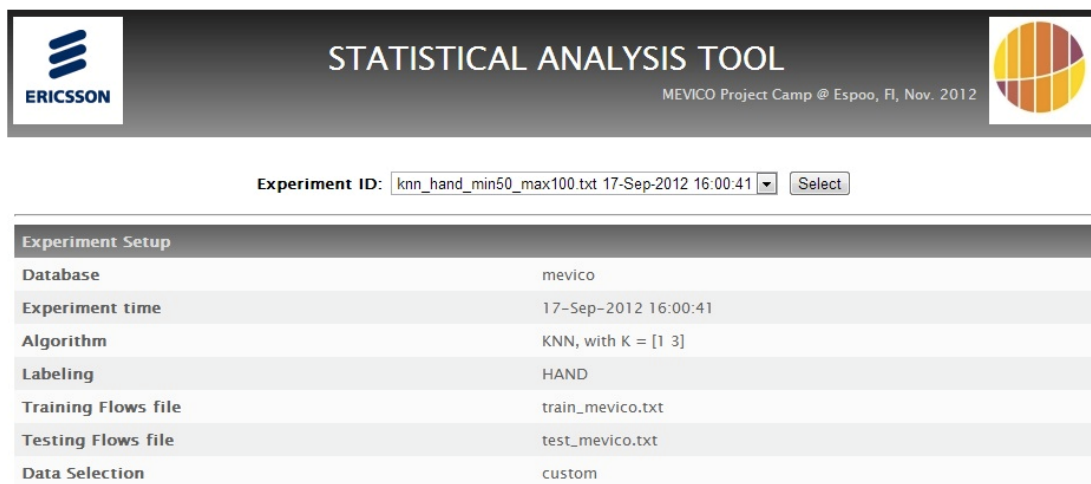
Conversational traffic: For conversational we merged the labels VoIP, Video Chat and IM. Initially the labels were decided by looking into the files generated by applications like Skype and QQ. To give a couple of examples, if the capture file was generated by Skype VoIP, we selected the largest flow of the capture and labeled it as “VoIP”. Similar for Video chat and IM.

However when we run the training set on the classifier and classified the test captures, our method was not successful in differentiating VoIP, Video chat and IM from each other, however it was able to differentiate these three from other application types much better. Therefore we decided to group them and name this group “conversational”.

We did not have any Gaming samples for the statistical algorithm. We did not have M2M samples either. M2M is expected to grow and may be divided into many sub-categories in the future.

Below figures are screen shots of the demo tool for the statistical classification algorithm.

Figure 4-4: Statistical analysis tool is the display where the information on the input files and the algorithm parameters can be seen.



Experiment Setup	
Database	mevico
Experiment time	17-Sep-2012 16:00:41
Algorithm	KNN, with K = [1 3]
Labeling	HAND
Training Flows file	train_mevico.txt
Testing Flows file	test_mevico.txt
Data Selection	custom

Figure 4-4: Statistical analysis tool

Figure 4-5: Training and test data for the experiment shows the statistics of the training and test samples. Some application types have numerous flows in terms of percentage of flows, however their percentage in the total size of the files may be less. This is very normal, for example P2P applications generate a lot of small sized flows, however this does not reflect on the byte size. Correct classification of large dimensioned flows is much more important than classification of small sized flows. From the figure, we can see that Conversational traffic was the major portion both in the training data and the test data. Video traffic holds the second major portion. Since this was generated by our sample captures, this will unlikely represent the distribution in a real network.

A. Training and Test Data for the Experiment

	Training data		Test data	
	Number of Flows	Total Size (MBytes)	Number of Flows	Total Size (MBytes)
NONE	551	19	0	0
P2P	164	110	128	63
VIDEO	42	442	19	138
CONV.	143	1265	49	312
WEB	11	25	4	36
TOTAL	911	1861	200	549

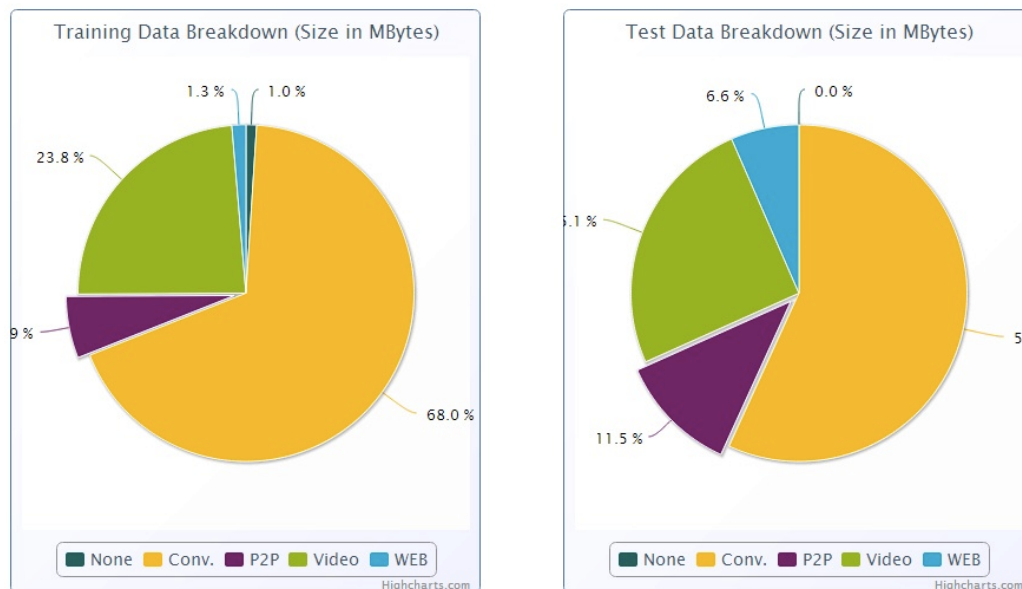


Figure 4-5: Training and test data for the experiment

Below figures, Figure 4-6: Confusion matrices and Figure 4-7 show the classification success rate of the algorithm on the test set after being trained by the training data.

Confusion matrix signifies the distribution of test application types onto classes by the algorithm. The more the diagonals are full, the better the results. Off diagonals represent misclassifications. Results have been provided both flow count based and megabyte based. Video and P2P seem to be highly successful. Even the megabyte based success rate is quite high for conversational. However there is more work to be done so that tests can be done with improving the training set. The training set and test set both had torrent protocol in abundance compared to the other protocols. Similarly Conversational class had more Skype samples than other application types. Improving the training set will improve the results and is an effort that has to be periodically spent so as to keep the algorithm up-to-date.

B. Confusion Matrices (Test Results)

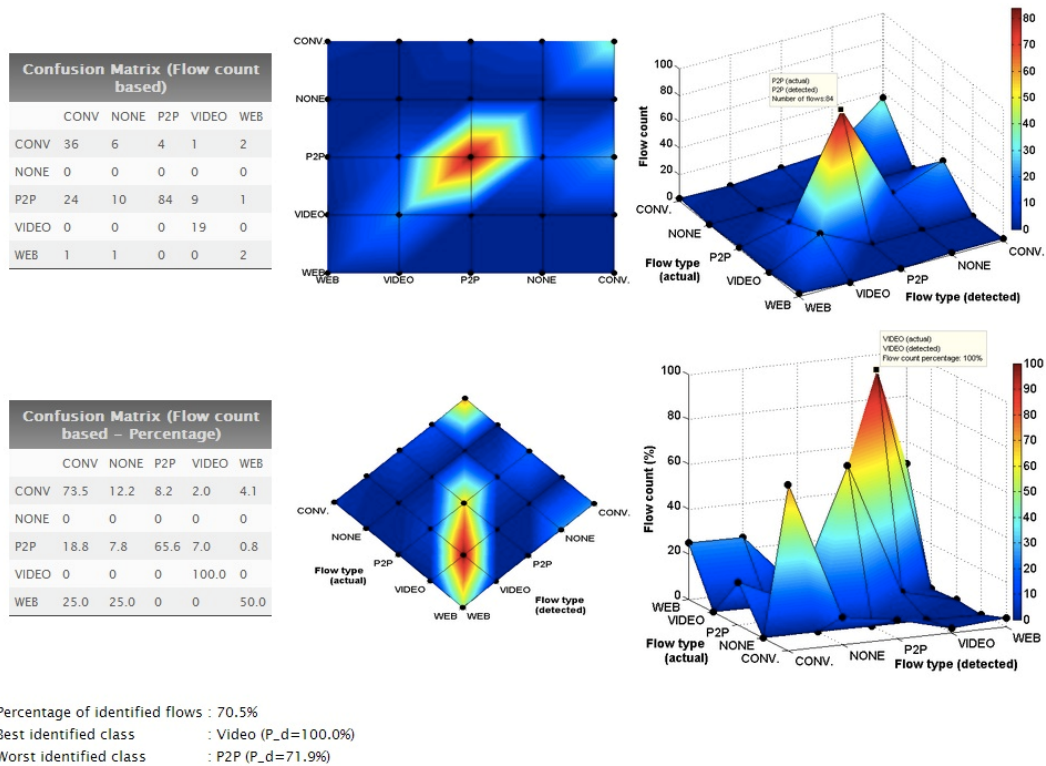


Figure 4-6: Confusion matrices

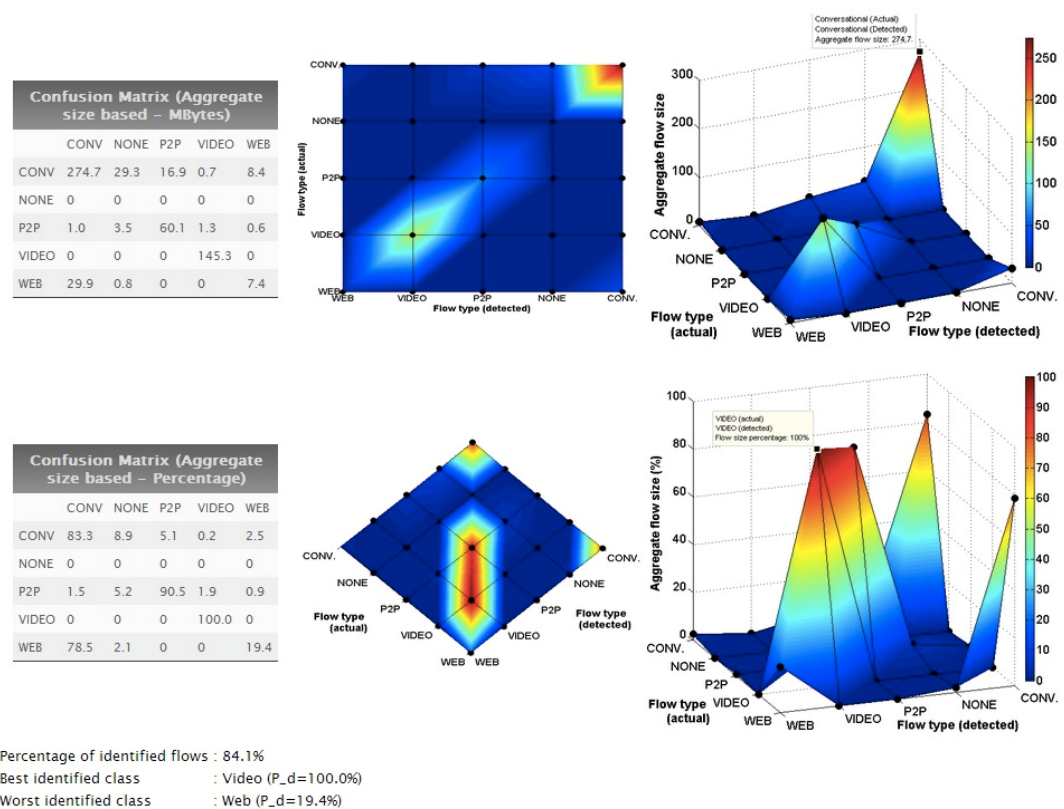


Figure 4-7: Confusion matrices

4.1.1.3.3 Broadband Reporting Tool

During the course of research for the statistical tool between Ericsson and Montimage, the high amount of collaboration came up with a second end result. As well as running the captures through a statistical reporting tool which classifies the flows in a very coarse fashion, we could obviously use DPI results to generate much more detailed reports which will help operators understand the usage in their network. We called this second form “Broadband Reporting Tool”.

With this tool, we worked on classifying the usage into the following categories:

- Video streaming
- P2P
- P2P streaming
- Conversational (contains IM, VoIP and video chat)
- Web
- Gaming, and
- M2M

Each category has subcategory reports such as:

For Videostreaming the applications generating the flows is being listed as youtube, dailymotion, facebook..

For P2P, the protocols used for P2P are provided.

For Web usage, the hosts and their popularity can be seen.

For Gaming, distribution of traffic among several popular games is provided.

P2P streaming has been handled as a separate case where the operator can merge into another category as well. This kind of streaming utilizes P2P protocols, however the behavior of this application is different from other P2P, no connection to multiple hosts. The QoS requirements of P2P streaming will be similar to other Videostreaming applications.

We did not have any M2M samples.

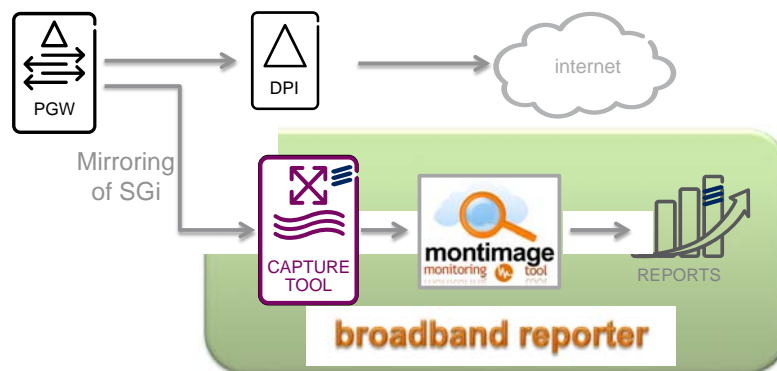


Figure 4-8: Architecture of the Broadband Reporting Tool

Almost 3 GB of data coming from more than 100 captures provided by Ericsson was analyzed by Montimage DPI during this work.

The classification rate was quite high.

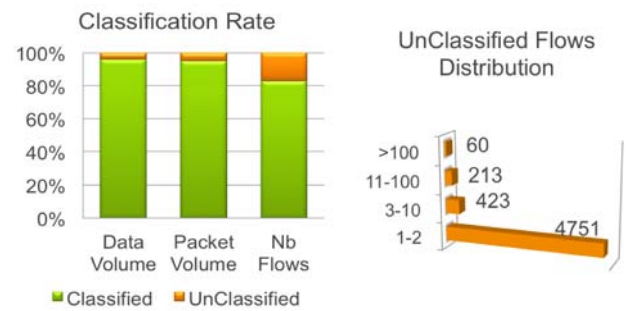


Figure 4-9: Classification success results of Montimage DPI over Ericsson provided data

Broadband Reporting Tool outputs can be seen in the following Figures which are screenshots.

Capture Analysis – Flow Statistics

	P2P	VIDEO STR.	P2P STR.	GAMING	CONV	HTTP	OTHER	TOTAL
Number of Flows (count)	8868	93	15	24	375	2959	9991	22325
Number of Flows (%)	39.72	0.42	0.07	0.11	1.68	13.25	44.75	100.0
Size (MBytes)	637.26	608.12	0.06	123.52	74.04	243.45	428.79	2115.23
Size (%)	30.13	28.75	0.0	5.84	3.5	11.51	20.27	100.0

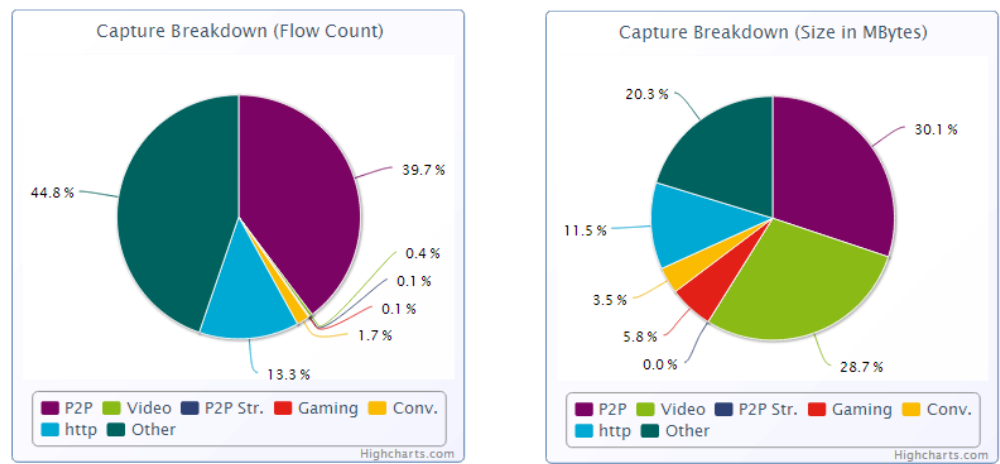


Figure 4-10 Breakdown of network capture onto applications

P2P Drill-down

	Number of Flows (count)	Number of Flows (%)	Size (MBytes)	Size (%)
gnutella	3194	36.03	71.36	11.2
manolito	2178	24.57	14.01	2.2
bittorrent	2637	29.74	514.29	80.7
iMESH	857	9.67	37.6	5.9
AppleJuice	0	0.0	0.0	0.0
Directconnect	0	0.0	0.0	0.0
TOTAL	8866	100.0	637.25	100.0

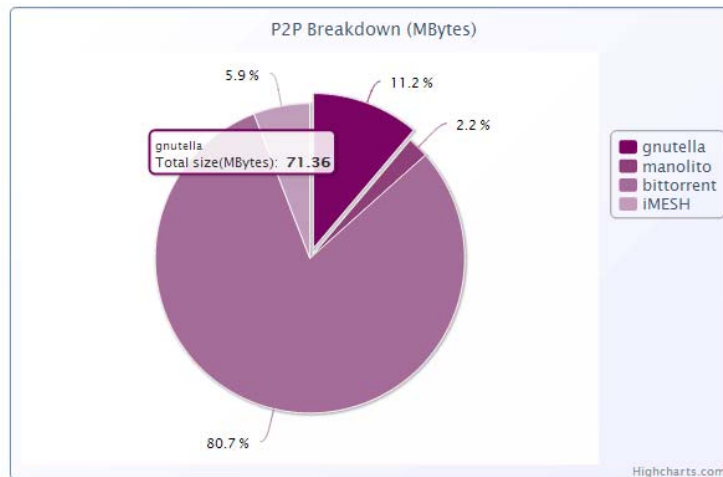


Figure 4-11: P2P Breakdown over various protocols



Video Streaming Drill-down

	Number of Flows (count)	Number of Flows (%)	Size (MBytes)	Size (%)
youtube	49	25.65	219.85	29.55
Dailymotion	44	23.04	388.27	52.19
iTunes	0	0.0	0.0	0.0
Facebook	0	0.0	0.0	0.0
Netflix	0	0.0	0.0	0.0
other	98	51.31	135.85	18.26
TOTAL	191	100.0	743.97	100.0

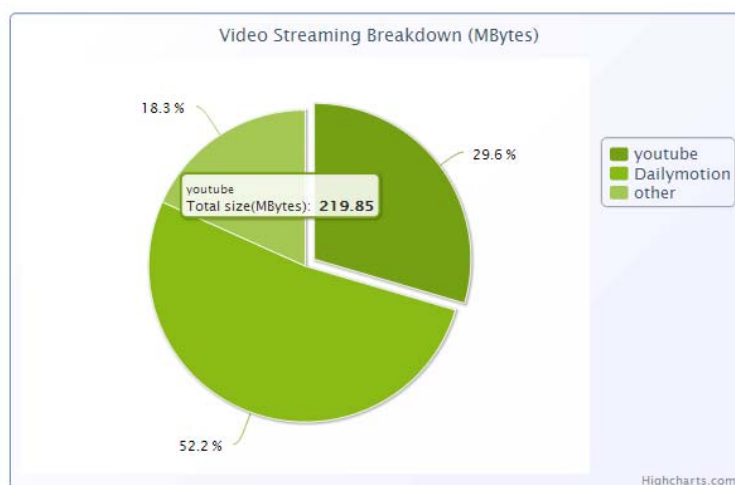


Figure 4-12: Video Streaming breakdown

WWW HTTP Usage : Top 5 domains

	google.com	bbc.co.uk/news	msn.com	facebook.com	gmail.com	TOTAL
Number of Hits (count)	36	24	18	12	6	96
Number of Hits (%)	37.5	25.0	18.8	12.5	6.3	100
Size (MBytes)	6.8	5.5	7.9	11.0	10.8	42
Size (%)	16.2	13.1	18.8	26.2	25.7	100

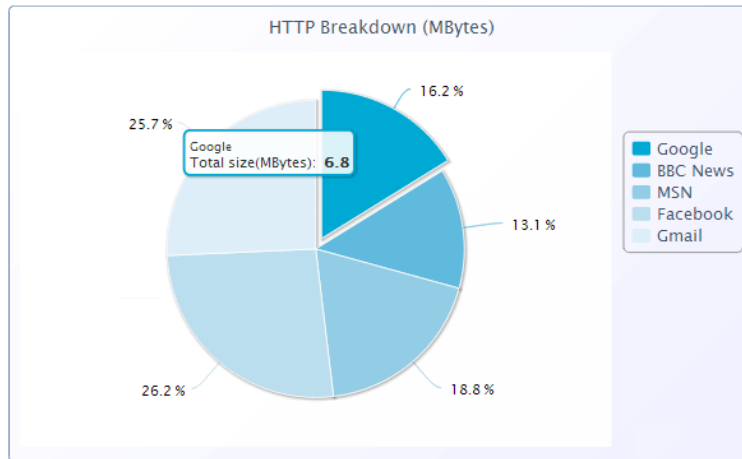


Figure 4-13: HTTP traffic breakdown



Conversational Traffic Drill-down

	Skype	MSN	GTalk	Yahoo	Jabber	Other	TOTAL
Number of Flows (count)	203	102	124	40	67	88	624
Number of Flows (%)	32.5	16.3	19.9	6.4	10.7	14.1	100
Size (MBytes)	159	66	111	24	54	45	459
Size (%)	34.6	14.4	24.2	5.2	11.8	9.8	100

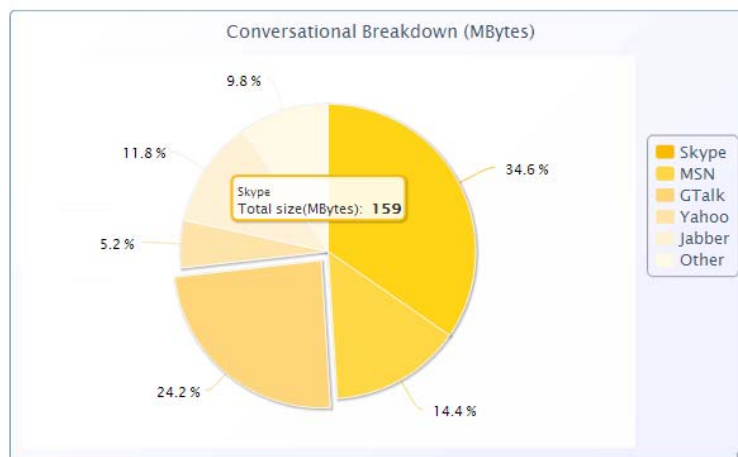


Figure 4-14: Breakdown of conversational traffic

Some special applications which may contribute to several of the above classes could be of special interest. With correct categorization of DPI results we can report them as well. Facebook can be the most popular example, so we developed Facebook breakdown.



Facebook Drill-down

	Image	Video	Conversational	Browsing	TOTAL
Number of Flows (count)	112	60	208	45	425
Number of Flows (%)	26.4	14.1	48.9	10.6	100
Size (MBytes)	12.4	56.2	29.6	20.8	119
Size (%)	10.4	47.2	24.9	17.5	100

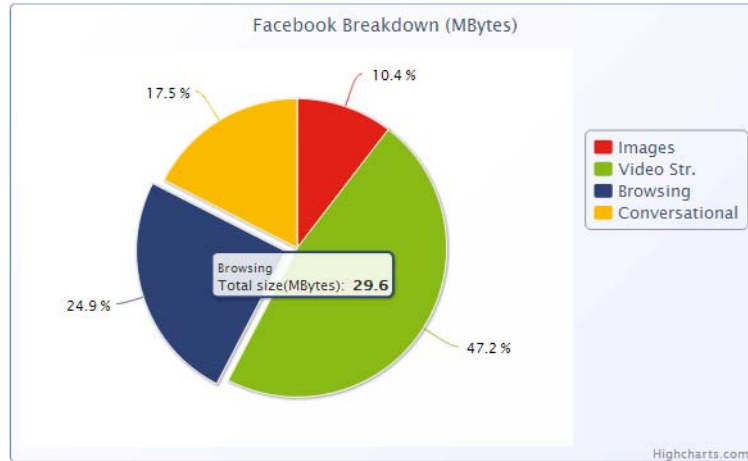


Figure 4-15: Facebook traffic breakdown over various usages

4.1.1.4 Challenges of traffic classification and QoS enforcement

It is a challenging task to classify applications accurately. None of the mentioned methods can provide satisfactory classification of all applications and therefore using together different techniques is typical in modern application classification modules (usually part of DPI systems).

In LTE, policy control is mandatory, meaning that policy enforcement is an essential requirement. This will require DPI functionalities, including application classification. For example, policy decisions can be initiated by Application Functions (AF) that might detect that a particular application is being initiated and notify the PCRF in order to get a decision. To identify the application in use, the AF can include or be linked to a classification function (DPI). We should note that the identification of managed applications (telephony, SMS) is simpler as the operator controls them.

Although, 3GPP standards specified a sophisticated QoS and bearer management model for LTE, it is expected that most Internet traffic will be assigned to the default bearer. In this case, application identification and classification will likely be needed to differentiate and manage internet traffic within the default bearer.

4.1.2 Application and user based differentiation

Differentiation of traffic flows for certain applications is increasingly requested and needs to be targeted on a flow or flow class model. This requires the above mentioned classification and detection efforts as well as several means for microscopic traffic management.

Commercial and Linux based routers are in general capable of such traffic manipulation, i.e. traffic shaping, dropping, delay management and bit manipulation.

In MEVICO it is envisioned to develop a microscopic traffic management framework, which derives the required traffic management actions from application QoS profiles associated with specific application behaviour (Skype/YouTube) models.

Starting with the application flow detection, it will be possible to lookup the essential QoS parameters thresholds for satisfying QoE levels and to apply the required actions in a distributed fashion. This concept is shown Figure 4-17.

This however requires a decision on the placement of detection and manipulation nodes within the operator network. The placement task will be solved through simulation as well as optimization efforts. Possible placement options are shown below in Figure 4-16.

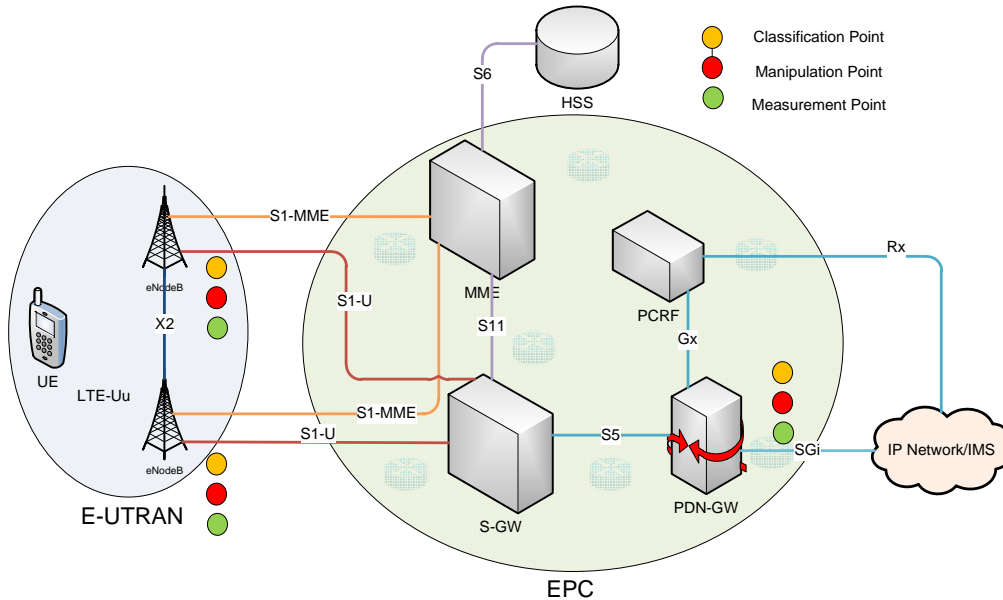


Figure 4-16: Possible points of presence within the network

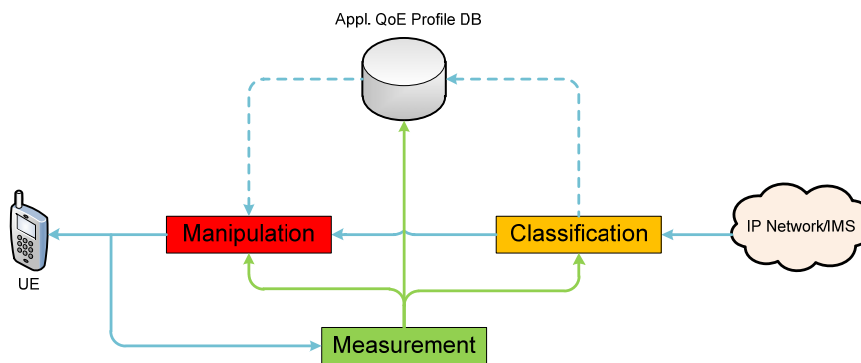


Figure 4-17: Measurement and control procedure

One of the major means for differentiation of applications is Quality of Service. Therefore here we focus on Quality of Service and how application and user based differentiation can be made.

4.1.2.1 ISAAR Framework [Eck12]

This section describes the ISAAR framework developed by CUT.

4.1.2.1.1 Framework Architecture

The ISAAR Framework has the logical architecture as shown in figure 2. The framework architecture is 3GPP independent but closely interworks with the 3GPP PCC. This independent structure generally allows for its application in non-3GPP mobile networks as well as in fixed line networks also. ISAAR provides modular service specific quality assessment functionality for selected classes of services combined with a QoE rule and enforcement function. The assessment as well as the enforcement is done for service flows on packet and frame level. It incorporates PCC mechanisms as well as packet and frame prioritisation in the IP, Ethernet and potentially the “Multiprotocol Label Switching (MPLS)” layer. Its modular structure in the architecture elements allows for later augmentation towards new service classes as well as a broader range of enforcement means as they are defined and implemented. Service Flow Class Index and Enforcement Database register the available detection, monitoring and enforcement capabilities to be used and referenced in all remaining components of the architecture.

ISAAR is divided into three functional parts which are the “QoE Monitoring (QMON)” unit, the “QoE Rules (QRULE)” unit and the “QoE Enforcement (QEN)” unit. These three major parts are explained in detail in the following chapters.

The interworking with 3GPP is mainly realized by means of the Sd interface [3GPP_TS_29.212] for traffic detection support), the Rx interface (for PCRF triggering as application function and thus triggering the setup of dedicated bearers) and the Gx / Gxx interface [3GPP_TS_29.212] (for reusing the standardized “Policy and Charging Enforcement Function (PCEF)” functionality as well as the service flow to bearer mapping in the BBERF).

Since ISAAR is targeting default bearer service flow differentiation also, it makes use of “Differentiated Services (DiffServ) Code Point (DSCP)” markings, Ethernet prio markings as well as MPLS “Traffic Class (TC)” markings as available. This is being enforced within the QEN by Gateway and Base Station (eNodeB) initiated packet header priority marking on either forwarding direction inside as well as outside of the potentially deployed GTP tunnel mechanism. This in turn allows all forwarding entities along the packet flow path through the access, aggregation and backbone network sections to treat the differentiated packets separately in terms of queuing, scheduling and dropping. No matter whether the entities are switches or routers.

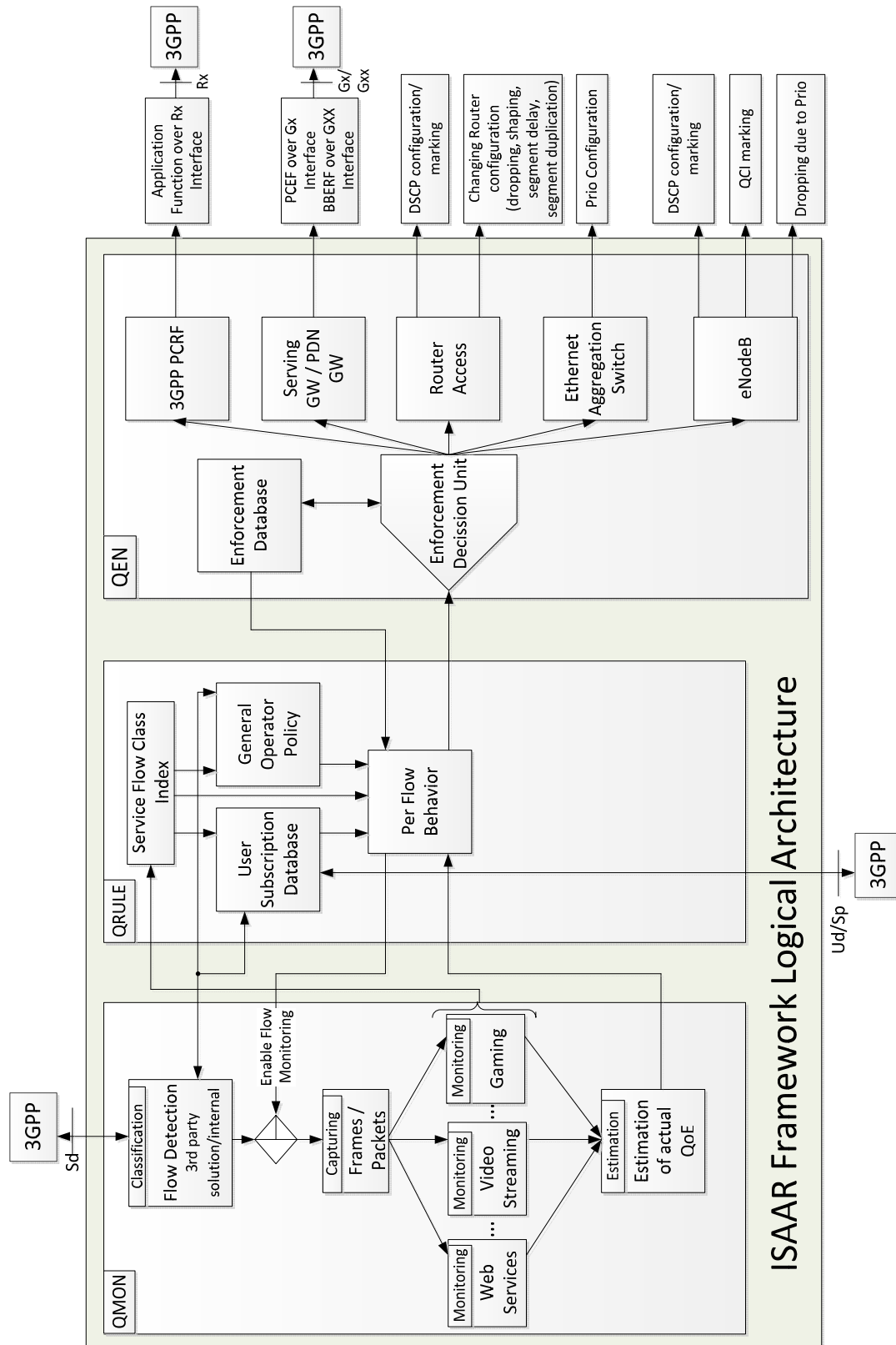


Figure 4-18: ISAAR Framework overview

The modular structure of the three ISAAR units (QMON, QRULE and QEN) allow for a more or less decentralized deployment and placement of the functional elements. Given the common network topology of today's mobile networks as shown in Figure 4-16, the placement of ISAAR components can be done on the potential locations (1) to (6).

QoE enforcement is the prominent functionality, which could profit the most from a distributed and harmonized deployment right from the access (1) into the core (5). It could also be deployed even behind the core towards the network interconnection to the public Internet. The QRULE unit seems to be sufficiently deployed in a centralized fashion - most likely number (5). The monitoring unit QMON is the

most difficult element for placement decision since this becomes a trade-off between service flow route pinning and the processing performance of the QMON device(s). Positioning QMON in (5) gives the advantage, that all traffic to and from the mobile node needs to go through this single point allowing for the complete monitoring of all exchanged service flow packets. However, the interface speed in this central location will become faster, which might require to decentralize the monitoring functionality into the aggregation or even access network part. GTP or MPLS tunnelling could still provide full packet view along a single path, but mobility effects need to be considered for this distributed detection and monitoring ISAAR mode of operation.

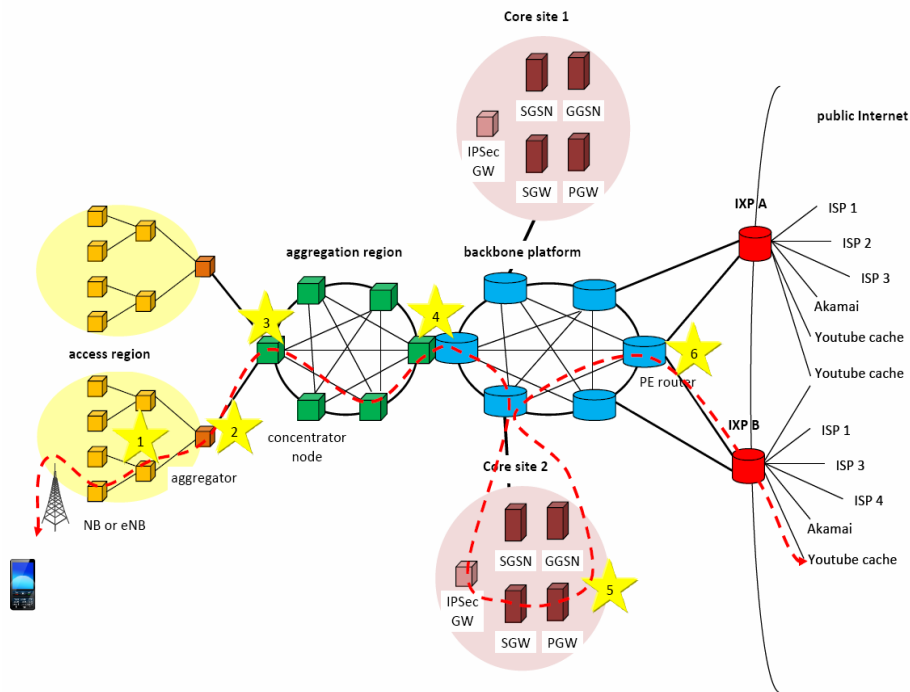


Figure 4-19: Placement options of ISAAR

4.1.2.1.1.1.1 QMON (QoE Monitoring)

Today's mobile networks carry a mix of different services. Each traffic type has its own requirements to meet the expectation of the user. The Internet Service Provider wants to satisfy the needs of their customers. Therefore the monitoring of the QoE of the users is necessary. Since the end user's quality of experience of a service is not directly measurable, a network based method is required, which can calculate a QoE "Key Performance Indicator (KPI)" value out of measurable QoS parameters. The most challenging and at the same time most rewarding service QoE estimation method is the one for video streaming services. Therefore, the first step of the ISAAR approach will focus on video quality monitoring and estimation, not limiting the more general capabilities of ISAAR for all sorts of service KPI tracking. YouTube is the predominant video streaming service in mobile networks and ISAAR is consequently delivering a YouTube based QoE solution first. Within this YouTube monitoring we are able to detect and evaluate the QoE of MP4 as well as "Flash Video (FLV)" in "Standard Definition (SD)" and "High Definition (HD)" format.

The flow monitoring which is used in the ISAAR Framework is explained in the following. However, before the QoE of a service can be estimated, the associated data flow needs to be identified. The next chapter explains the flow detection and classification.

Flow Classification

The ISAAR Framework is meant to work with and without support by an external "Deep Packet Inspection (DPI)" device. Therefore it is possible to use a centralized DPI solution like the professional devices provided by Sandvine [SAN12]. For unencrypted and more easily detectable traffic flows, it is possible to use a cheaper and more minimalist DPI algorithm which is provided within the ISAAR Framework. The two possibilities could be seen in Figure 4-16. For a distributed solution, the DPI nodes could be located on location (1) to (6), in a centralized case, location (5) or (6) have to be chosen. In a distributed classification architecture, the classification load could be managed by each node. In a first

demo implementation, the classification is limited to “Transmission Control Protocol (TCP)” traffic, focussing on YouTube video stream detection within the traffic mix.

In the centralized architecture the flow detection and classification is most suitably done by a commercial DPI solution, in the demonstrator a Sandvine PTS8210 is used. In this case the measurement nodes have to be informed, that a data stream was found and the classification unit has also to tell them the “five tuple”. Contained in the five tuple are the source and destination IP address as well as the source and destination port, the last information element is the used transport protocol. The measurement starts, as soon as the node gets the identification information of the flow.

Flow Monitoring

The flow monitoring within the ISAAR Framework is application specific. For each service, which should be monitored, there has to be a specific measurement algorithm. The first part of the monitoring section is the Video QoE estimation (e.g. for YouTube). Like all for the framework planned measurement algorithms the video estimation is a network based algorithm. The advantage is that they are working transparently and fully independent from the user’s end device. Therefore, no tools have to be installed and no access on the end device has to be granted.

The approach presented is focusing on video stalling events and their re-buffering timings as a quality metric for the QoE instead of fine grained pixel and block structure errors. To determine the number and duration of re-buffering events it is necessary to comprehend the fill level of the play out buffer at the client. Focusing on YouTube video incurs TCP encoded HTTP streaming transport.

Our method performs the QoE estimation based on the measured TCP segments of the video stream at the observation point. In the following we describe 3 variants of our method - an exact method, an estimation method and a combination of these.

For all methods the following steps have to be carried out in advance: (1) the video flow needs to be identified within the traffic mix, and (2) the TCP segment information and the TCP payloads of the video flow have to be extracted.

Exact Method:

The actual play out time is extracted from the decoded video and compared with the timestamp of the respective TCP segment. Out of this comparison the fill level of the play out buffer can be estimated. This includes the processing of the initial buffering phase, the stalling detection by buffer depletion events as well as the correct calculation of re-buffering times.

Estimation Method:

The estimation method is a variation of the exact method aiming for a better processing performance. The idea is to decode the header of the streamed video only. The collected video information in the header includes the respective size and duration information of all subparts (chunks). The estimation algorithm calculates the fill-level based on those chunk sizes and the observed amount of data streamed. This calculation yields the number and duration of re-buffering events. Note, that there is a trade-off between processing speed-up and accuracy.

Combination of the two Methods:

The last variant of the algorithm tries to combine the gained speed-up of the second variant with the accuracy of the exact algorithm. This is obtained by dynamically adopting the processing mode (exact mode/estimated mode) to the experienced throughput. The adoption is based on a single threshold value of the buffer fill-level: the exact method is used only if the buffer fill-level is below the threshold.

Note, that the precision of all 3 algorithms can be further improved by using the timestamp of the ACKs instead of the timestamp of the TCP data segments for the buffer fill-level calculation.

Location aware monitoring

Due to the fact that it is probably not possible to measure all streams within a provider network a subset has to be assigned in a random way. But the distribution of the samples could be mapped to the tracking areas. So it is possible to draw a random set of samples which is normal distributed to all tracking areas. If it is also possible to map the eNodeB cell “Identifications (IDs)” to a tracking area, it becomes possible

to draw the samples in a regionally distributed fashion. With the knowledge of that it could be decided whether a detected flow is monitored or not due to the respective destination region. If there are enough samples within the destination area of the flow, further flows will not be selected for measurement. If there are no or few measurements in this area, the flow would be observed.

4.1.2.1.1.2 QRULE (QoE Policy and Rules)

The QRULE gets the flow information and the estimated QoE of the corresponding stream from the QMON entity. It also contains a service flow class index in which all measurable service flow types are stored. In interaction with the user subscriber Database and the general operator policy, where the operator's policy for each service and the information for what service a user has subscribed is stored, the flow behaviour is appointed. Also the enforcement database within the QEN, which is explained in chapter 6, is taken into account. In combination with all this information the QRULE maps the KPIs to the forwarding and routing rules for each data stream managed by ISAAR. The "Per Flow Behaviour (PFB)" is implemented by marking of packets and frames. Therefore the each PFB has to be specified. Table 4-1 shows an example of PFB configuration settings for e.g. video streaming, voice traffic and Facebook traffic.

Media Type	Key Performance Indicator	IP DSCP	Ethernet Prio	MPLS Traffic Class	3GPP QCI	Action
Video	Buffer Level in Sec. $Th1 < t < Th2$	CS5 101 000	101	101	6 (or 4)	Mark in S/P-GW and eNodeB with high priority
	Buffer Level in Sec. $t < Th1$	"Expedited Forwarding (EF)" 101 110	111	111	1	Mark in S/P-GW and eNodeB with highest priority
	Buffer Level in Sec. $Th2 < t$	"Best Effort (BE)" 000 000 or even Lower Effort LE 001 000	000	000	9	Mark in S/P-GW and eNodeB with default priority or even start dropping packets
Voice	Delay in ms	EF 101 110	111	111	1 or 2	Mark in S/P-GW and eNodeB with highest priority or even Create dedicated bearer with QCI 1 or 2
Facebook	Page load time	CS5 101 000	101	101	6	Mark in S/P-GW and eNodeB with high priority
...						

Table 4-1: Per Flow Behaviour table

In the video section are three possible modes which are depending on the buffer fill level calculated in the QMON. According to the information from QoE monitoring different markings are chosen. In the example shown in Figure 4-20 the two buffer fill level thresholds are defined to $th1 = 5$ seconds and $th2 = 25$ seconds. If the QoE is poor, that means the video buffer fill level is below Threshold 1 ($t < th1$), the EF class or the equivalent class of the other technologies is used to improve the video QoE. Lies the fill level between Threshold 1 and 2 ($th1 < t < th2$) a DSCP value like CS5 (101 000) should be chosen, because the QoE is ok and needs not to be treated in a special way. For the third case if the fill level exceeds Threshold 2 ($th2 < t$) QRULE has to choose a DSCP value with a lower prioritization (like BE 000 000 or LE 001 000), so the freed resources could be occupied by other flows.

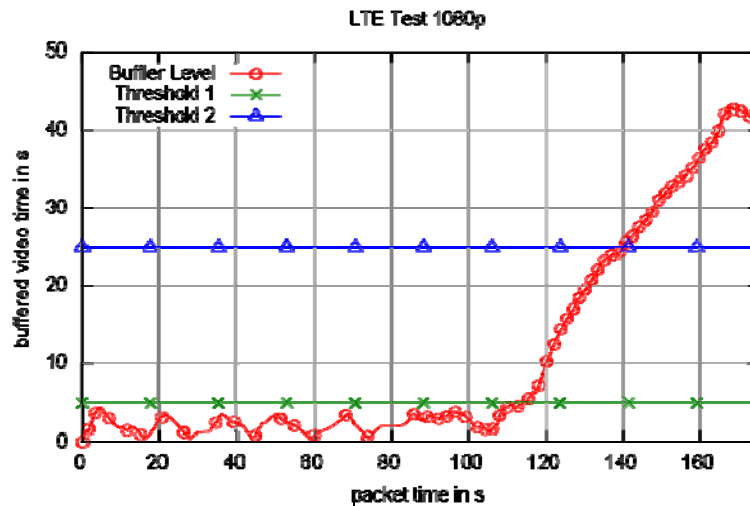


Figure 4-20: Per flow Behaviour dependent on the buffer fill level in a YouTube example

QRULE also decides which kind of marking is deployed depending on the available technology. So it is possible to use the DSCP marking for IP routing, Prio for Ethernet forwarding, the MPLS class for “Label Switched Path (LSP)” switching and the QCI tunnel mapping for 3GPP. Due to the reason that these mechanisms are used in combination in provider networks, there must be a consistent mapping between them. This mapping is also done by the QRULE. Further details on the mapping can be found in [Knoll12]

For future investigation ISAAR is prepared to incorporate the interworking of GTP and MPLS LSP tunnels in a transparent fashion. Further details on the interworking can be found in [Wind08].

4.1.2.1.1.1.3 QEN (QoE Enforcement)

The third function block in the ISAAR Framework is the QoE Enforcement. In this block the flow manipulation is done. For example if there is an internet service data stream which is estimated with a low QoE then the QEN has to react and e.g. prioritize the flow. To do this we assume some methodologies to influence the transmission of the involved data frames or packets. One possibility is to take advantage of a PCRF/PCEF with dedicated bearers where it is applicable and trigger the setup via the Rx interface.

The second method we propose to be located within the eNodeB and the “Serving Gateway/Packet Data Network Gateway (SGW/PGW)”. It is based on layer 2 and 3 marking within the GTP tunnel as well as outside. How the marking is transferred from inside the GTP to outside is discussed in detail in chapter 5. With the GTP outside marking the stream can be prioritized over other streams along the forwarding and routing path using commonly available priority and DiffServ mechanisms. So the stream is preferentially handled by the network elements without any new configuration within those elements. The marking has to be done by the SGW/PGW for the downstream and the eNodeB has to mark the upstream packets. To be able to mark all packets of a flow, the flow information (five tuple) must be transmitted from the QMON block to all involved elements in this case the SGW/PGW and the eNodeBs which the flow will pass through. This could e.g. be realized via the “Mobility Management Entity (MME)” and the flow state could automatically be transferred during handover using the standard user state procedure.

The outer tunnel marking has also to be transferred to the “Internet Protocol Security (IPSec)” so that the priority of an encrypted stream can also be changed. Therefore the DSCP value of the outer tunnel IP packet header is set to the same value. This leads to the possibility to handle encrypted traffic streams without decryption. The network element need not to know what kind of flow is within the tunnel they only handle the IP packets by their DSCP configuration.

The marking mentioned above has to be done within IP, Ethernet Priority, MPLS Priority and the QCI classes. To get a comprehensive QoE Enforcement, the flow has to be classified and measured in the QMON, the priority of that flow has to be determined by the QoE Ruler and then the QoE Enforcement takes place and does the marking. But the marking has to be valid in the whole operator’s network, where the mentioned priority markings were used in a mixed way. To overcome that, the markings have to be converted to each other which is also explained in detail in chapter 5. Marked packets or frames could be routed or forwarded with operator configured per hop behaviour, which results in different queuing and dropping strategies. With this option the QEN does not have to change the router or switch configuration within the operator’s network. Because such priority based forwarding and routing is handled

automatically by prio enabled Switches and “Label Switch Routers (LSRs)” as well as DSCP enabled routing devices.

But the ISAAR Framework should be also able to do a fully automated router configuration [Eck10] . For that case the enforcement function optionally changes the router behaviour for a specific flow. Thus the packet dropping is influenced. To do this the QEN has to be aware of the actual router configuration and has to change it in a way that the stream’s needs are met. After the configuration is changed it must be transferred back onto the router. There are two conceivable ways how the QEN could be aware of the actual router configuration. The first one is to read the information from the router in at first. But with this option the signalling load is increased and it takes a lot of time. A second approach is that the router configuration of all routers is known in a configuration database. In this variant ISAAR only changes the configuration send it to the corresponding devices and save the new configuration in this database.

4.2 End-to-end QoS

The performance of wireless cellular networks is often evaluated in terms of parameters such as the spectral efficiency or the outage probability in academic research and within 3GPP. However, from a network operator point of view, it is important to measure and calculate KPIs in terms of QoS parameters such as latency, jitter, packet loss rate, throughput etc. depending on the application type (such as voice, video, data, control signaling, IT traffic, etc.), from which SLA compliance and end user perceived QoE. This relation is crucial for minimizing the network cost while ensuring QoS as demanded by applications for business and residential users.

4.2.1 End-to-end (E2E) QoS in 3G

3GPP defined e2e QoS in Release R99 based on four services and traffic classes:

1. Conversational (e.g. voice),
2. Streaming (e.g. streaming video),
3. Interactive (e.g. web browsing),
4. Background (e.g. background download of emails, files etc.)

In HLR (Home Location Registrar), there are some QoS related parameters such as GBR (Guaranteed Bit Rate), MBR (Maximum Bit Rate) and THP (Traffic Handling Priority), ARP (Allocation and Retention Priority). There are three levels of ARP, 1- high, 2-medium, and 3-low.

The scheduling of packets is done based on SPI (Service Priority Index). There may be a different number of SPI levels. In the Node-B scheduling process, RABs (Radio Access Bearers) are mapped based on SPI with an operator definable weight on each of 15 SPIs (Scheduling Priority Indicator).

Node-B shall use these different SPI levels with appropriate scheduling algorithms (e.g. maximum C/I, Proportional Fair, minimum GBR, etc) to differentiate individual HSDPA flows, taking into account both radio conditions, resources and call priorities.

The following topics have been detailed in D 4.3.1:

- Bearer concept for QoS support
- Types of bearers
 - QoS parameters of the bearer concept
 - Applying QoS parameters and bearers in LTE
- Related QoS standards for IP and other packet networks (MPLS, Ethernet)
 - QoS Mechanisms in IP networks: IntServ, DiffServ
- Challenges of the 3GPP Architecture for ensuring E2E QoS control for LTE
- An example for standardized QCI characteristics

4.2.2 Services, KPIs and implementation steps for E2E QoS parameters in the network

4.2.2.1 Exemplary services

Voice refers to VoIP bearer traffic only and does not include call-signaling traffic.

Interactive video refers to IP video-conferencing and combines delay constraints as for VoIP with high variable bandwidth demand.

Interactive online gaming has extreme demands for non-noticable delay.

Streaming video is either unicast or multi-cast uni-directional video which can make use of buffering.

Best effort bulk data is intended for background, non-interactive traffic flows such as large file transfers, content distribution, database synchronization, back-up operations and email (e.g. file transfers and downloads via ftp, P2P, etc).

Transactional data is intended for foreground, user interactive applications such as database access, transaction services, IM and preferred data services.

Call-signaling class is intended for voice and video signaling traffic such as Skinny, SIP, H.323, etc.

Network management is intended for network management protocols, such as SNMP, Syslog, DNS, etc.

Routing data exchange is intended for IP routing protocols such as BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), etc.

4.2.2.2 Common KPI parameters for different applications

Data applications: Typically best-effort services, characterized by variable bit rates, being tolerant to some loss and latency before the user perceives poor quality

- Transaction latency (including time-to-first-byte and time-to-last-byte of data)
- UL/DL throughput of data [Mb/s] or measured as transactions per second
- Concurrent transactions
- Loss rate, Re-transmissions - TCP retries
- Connection latencies and failures
- Service availability (as a percentage, e.g. demand for the five nines 99.999%)

Conversational applications: Real-time services requiring a constant bit rate. Voice services are sensitive to latency and jitter, but tolerate of some packet loss.

- Maximum and average jitter
- Delay bounds
- Mean opinion score (MOS)

4.2.2.3 Steps for determining QoS parameters for a given network

Step 1

Simulate each UE with applications such as example services mentioned above and associate them to specific QCIs (bearers) valued from 1 to 9. Distinguish subscribers (Platinum, Gold, Silver, Bronze or emergency) and data rate values (5Mbps, 20Mbps, 100Mbps, etc.), and map them to QCIs (in HSS subscriber's profile). Use also MBR to create different levels of services (some exemplary services are also given above) in HSS subscriber's profile. In addition, the application differentiation concept might be configured.

Step 2

For validation of DiffServ prioritization in the IP transport network, test QCI-to-DSCP mapping. The eNodeB on one side of the LTE network and the PDN-GW on the other side must map QCIs to DSCP. This mapping between the bearer-aware networks and the transport network (DSCP/802.1p/EXP mappings) must be tested for accuracy.

Step 3

Create congestion at radio and transport networks with varying traffic profiles and distinguish between them by inserting heavy load into the network. Measure and report behavior and KPIs from IP and Ethernet transport equipment (IETF, MEF) and from 3GPP network elements. The simulation can also be implemented with traffic simulators such as load generators [DevoTeam] (see next subsection for an example usage of load generator for generating signalling load).. It's only when the network becomes congested and there is competition for resources that we find out if QoS, policy and prioritization are working properly.

Step 4

Measure and report KPIs for each QCI (bearer). The network operator defines the KPI expectations associated to each specific bearer. Most common KPIs are also given above for data and voice traffics. The carrier measures and reports KPI's for each QCI over time and with different traffic and subscriber mixes to observe whether they are within the defined threshold limit.

4.2.2.4 Signaling traffic analysis tests using load generator: An example for e2e signaling traffic

Before applying an optimization framework in a real network environment, simulation tools that can produce load and real data traffic via building appropriate simulation models in accordance with 3GPP signaling protocols are needed. This can verify the behavior of network components under different loads, can discover each bottleneck spots in the network and can give intuitive information about end-to-end QoS state. Load generator is one such end-to-end simulation tool. It can provide a cost effective traffic simulation for testing GSM/GPRS, WCDMA/UMTS and LTE/EPC networks.

Load generator

Figure 4-21 is the block diagram of typically used load generator in a mobile operator's network architecture and testing department (SITT mobile services test platform product's load generator is used for this example [DevoTeam]). The greatest advantage of a load generator is that it can produce real traffic data with the desired amount of load and different packet traffic characteristics in real time. Therefore, prior results can be emulated smoothly in order emulate the real network environment considering all possible changes that can occur in a network infrastructure. Figure 4-21 represents the network elements that can be emulated by the load generator. The SITT load generator can operate in two modes: SGSN_MME and GGSN operation modes. Basically in load generators, user-SGSN-GGSN-Internet traffic can be generated with all the signaling messages (attach, PDP (Packet Data Protocol) activation, etc) that comply with 3GPP standards. Therefore, load generators are an easy way to test and utilize the network elements in a cost efficient and risk-free manner.

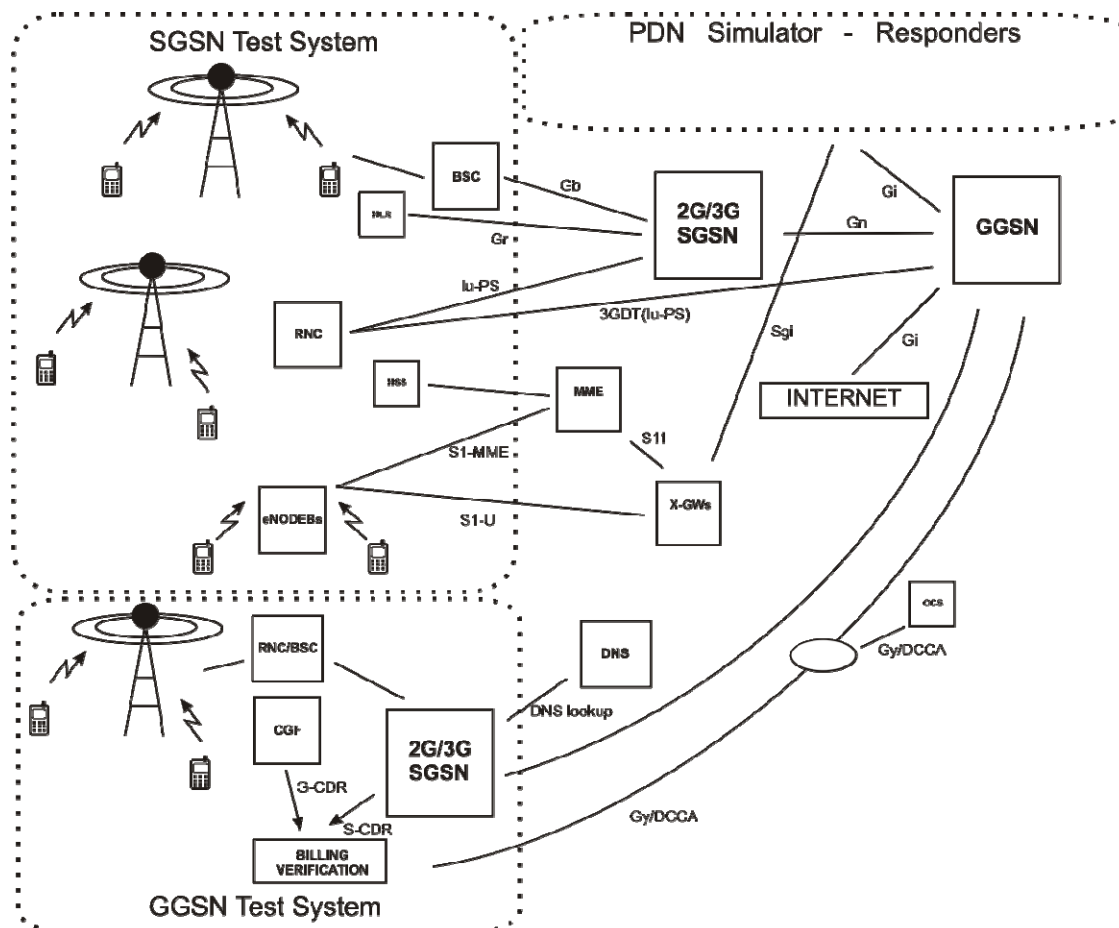


Figure 4-21: Load generator block diagram [DevoTeam]

Different possible test architectures can be tested using a load generator. Typical network elements in a mobile operator's core network infrastructure are drawn in Figure 4-22. Similarly, another network architecture is shown in Figure 4-23.

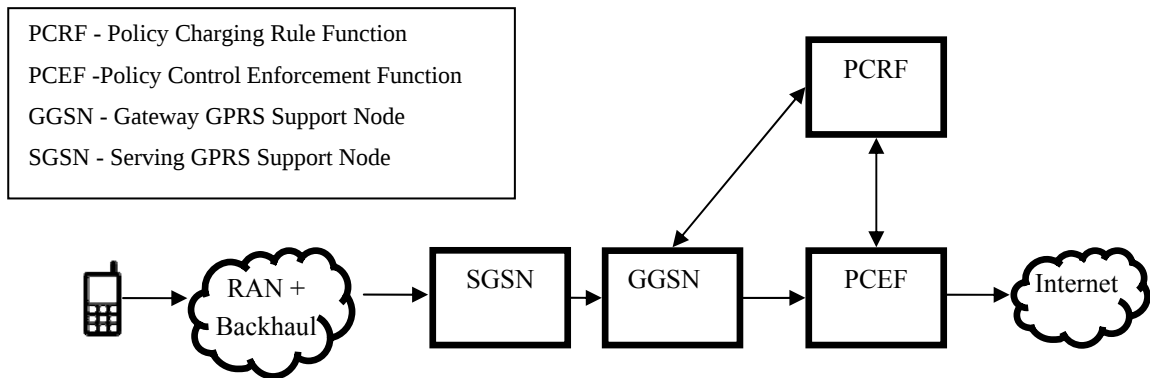


Figure 4-22: Test architecture 1 (separate)

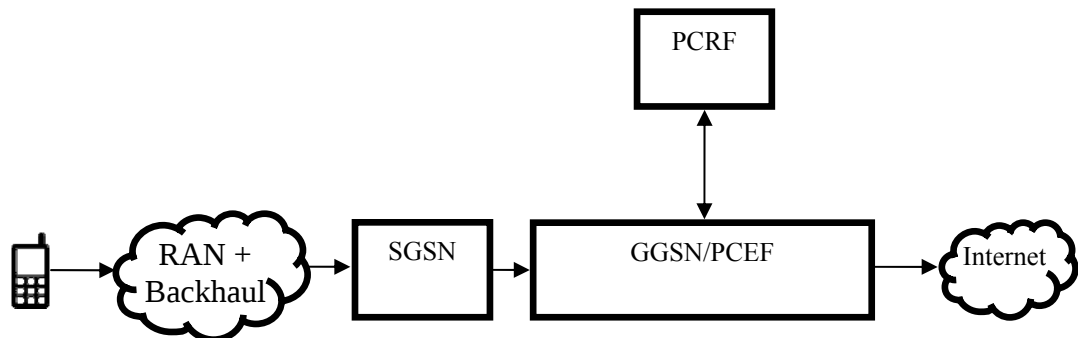


Figure 4-23: Test architecture 2 (flat)

In order to compare the amount of signaling (such as “create PDP context request messages”) for these two different architectures, load generator is operated in SGSN_MME operation mode. SGSN_MME mode is implemented according to 3GPP TS 24.007 v5.2.0 and 3GPP TS 24.008 v6.16.0 [DevoTeam]. Figure 4-22 shows the network architecture where GGSN and PCEF network elements are separate, whereas Figure 4-23 shows it as single component (i.e. flat architecture) in the core network.

Test Results

Figure 4-24 and Figure 4-25 show the signaling messages into PCRF from GGSN and PCEF network elements when “create PDP context messages” are initiated for different architectures of Figure 4-22 and Figure 4-23 respectively. At the beginning of test procedure, the number of subscribers is selected to be 200 and this number is increased systematically until system can no longer support the number of new comers and the performance deteriorates. The upper limit for the amount of simultaneous subscriber’s “create PDP context request messages” depends on the network architecture. If this upper limit is reached within a specific architecture, additional number of subscribers will be rejected for further attachments. Figure 4-24 and Figure 4-25 show the approximate number of subscribers that can be supported for each different architectures (Figure 4-22 for separate architecture and Figure 4-23 for flat architecture). In separate architecture, the number of simultaneous subscribers that can be supported by the system is 250 users per second, whereas it is 500 users per second. This result clearly shows that separate architecture (Figure 4-22) has approximately two times more extensive signaling messages compared to flat architecture (Figure 4-23). Uniting PCEF and GGSN network elements in a single entity will support more simultaneous subscribers compared to separate architecture, since the amount of signaling into PCRF is nearly one-half.

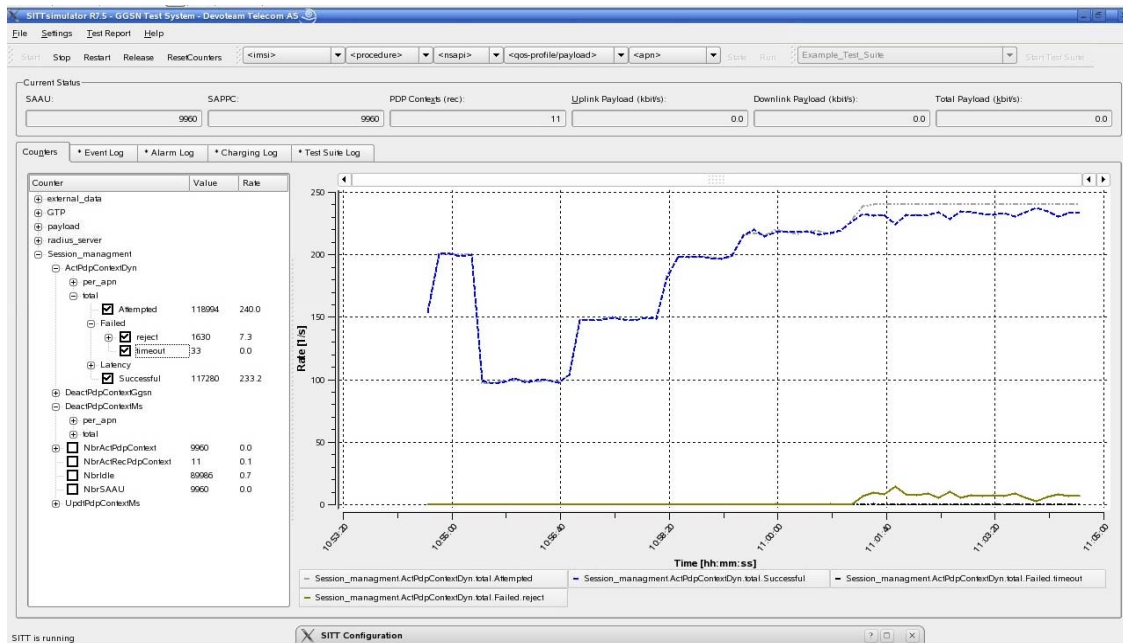


Figure 4-24: Gx interface PCEF-GGSN separate architecture

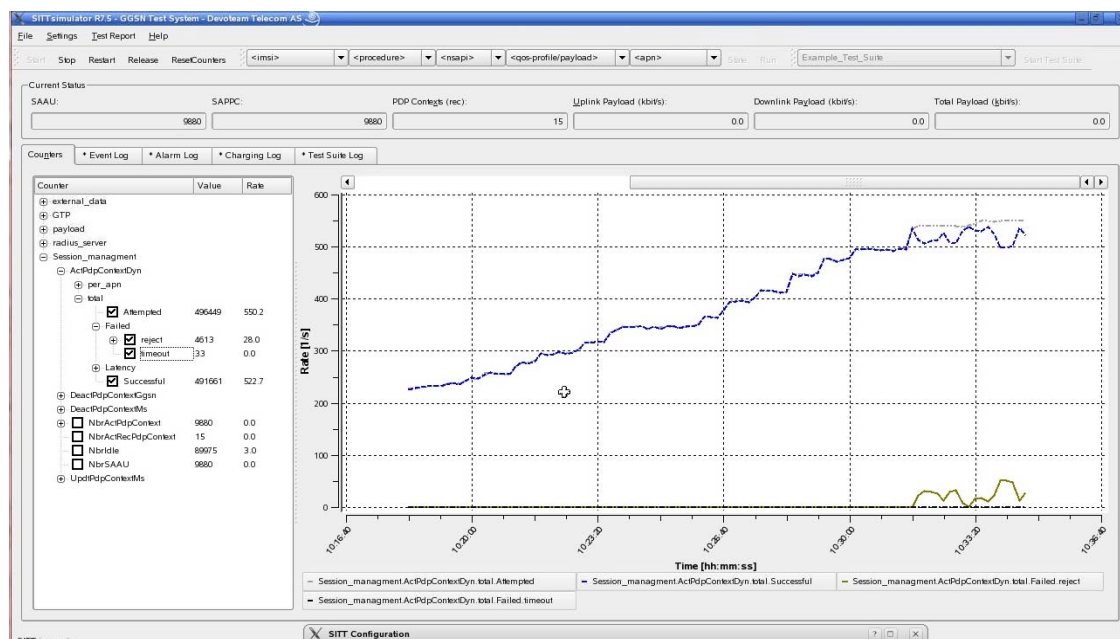


Figure 4-25: Gx interface PCEF-GGSN flat architecture

Another topic of importance, challenges & solution approaches for inter-provider end-to-end QoS has been covered in D 4.3.1.

5 Improved resource selection & caching

5.1 Resource selection

Resource selection is one of the key functional mechanisms to select best suitable resource in P2P and CDN networks. Objectives and major concepts have been presented in D 4.3.1.

5.2 Internet-based Content Distribution via CDN and P2P Overlays

Following topics have been detailed in D 4.3.1:

- Content delivery networks (CDN)
- Peer-to-peer networks (P2P)
- Transport paths of CDN and P2P overlays on broadband access infrastructure
- Comparison of delays on CDN and P2P transport paths
- Summary of characteristics for content delivery in CDN and P2P networks
 - Network and Application Layer Approaches for Short Transport Paths
 - Application layer positioning approaches
 - Traffic engineering support by information servers in current IETF standardization

Major topics in content caching have also been investigated in D 4.3.1:

- Functional analysis of Content Caching
 - Non-transparent vs. transparent caching
 - In-line vs. out-of-band caching
 - Caching metrics
- Caching efficiency for web-based content
 - Zipf laws to estimate requests for popular content
 - Measurement of access patterns and evaluation of the effect on caching

Here an ALTO extension is being detailed as finalized research.

For Combined CDN, caching and P2P overlay approaches, D 4.3.1 should be referred as well.

5.2.1 ALTO extension proposal for UE with scarce resources and/or intermittent connection

5.2.1.1.1 Motivation

The Client/Server IETF protocol ALTO, see [AL11] provides abstracted information on the transport topology underlying the overlay network of applications such as P2P and CDN. This information includes abstractions of network maps, cost maps and endpoint costs. Abstraction is done by

- Providing topologies of “network locations”, specified by the managing ISP and corresponding to host groups of heterogeneous levels in the Internet hierarchy and
- Associating ISP defined “routing costs” among these network locations.

The current ALTO protocol provides a unique value for the requested cost type, and if up to date values are needed they must be requested as often as the value is changed. However, frequent ALTO transactions for updates are costly. In some cases though the cost value changes are predicted, in particular for the sake of traffic regulation, and having a set of predicted values beforehand would be highly beneficial to the applications and end systems relying on the ALTO service.

In particular, ALTO supported applications such as content delivery spatially shift traffic between network regions in order to lower routing costs for ISPs and regularly move content across their caching nodes to better map to the demand; many non-real time applications have a degree of freedom on *when* to “use a resource”, given that

- a “resource” is a content file or a computation resource stored in a data center and

- "use" a resource means for example, do a content transfer between caches, access a service, use a physical server for a virtualized application or do time shifted content delivery.

Nowadays, popular applications ran on UEs in wireless network such as content delivery and clouded applications become a challenge for the network and the UEs due to the scarcity of resources and challenged network access. Application clients on end systems with limited access to data centers and/or to the network or using resources scattered around the world need to schedule their access to resources or need to figure out when resource transfer or access costs may change. In some cases of non real time applications, this cost is predictable over a given number of time slots.

ALTO Cost Schedule

- Extends ALTO Cost values in time horizon
 - Specifies time slots (hourly slots) over a period of time (24 slots)
- New Cost Mode = "schedule,,
- Cost Mode attributes


```
"cost-scope": [{"unit": ["hour", 1], "size": 24,
                  "begin": 0, "time zone": "UTC",
                  "lastupdate": "mm/hh/dd/mm/yyyy",
                  "nextupdate": "mm/hh/dd/mm/yyyy"} ]
```
- ALTO cost values in Schedule mode can be used
 - As historic or predictive information to estimate the expected QoE
 - To accordingly schedule transfers or access to application resources (contents, services...).
 - To schedule ALTO requests, since the value change frequency is known

5.2.1.1.2 Use case 1: End systems with connectivity or access to datacenters that is **variable and predictable**

Applications such as remote learning, enterprise database update, remote distributed computation and thus wish to schedule their connection to application Endpoints.

Another use case that benefits from the availability of multi-timeframe cost information is based on applications that are limited by their connectivity either in time or resources or both. For example applications running on devices in remote locations or in developing countries that need to synchronize their state with a data center periodically, in particular if sometimes there is no connection at all. One example applications is enterprise database update, remote learning, remote computation distributed on several data center endpoints.

Wireless connectivity has a variable quality or may even be intermittent. On the other hand, the connectivity conditions are often predicable. For non real time applications, it is thus desirable to provide ALTO clients with routing costs to connection nodes (i.e. Application Endpoints) over different time periods. This would allow end systems using ALTO aware application clients to schedule their connections to application endpoints.

Another challenge arises with end systems using resources located in datacenters and trading content and resources scattered around the world. For non-real time applications, the interaction with Endpoints can be scheduled at the time slots corresponding to the best possible QoE value. For instance, resource Ra downloaded from Endpoint EPa at time t1, Resource Rb uploaded to EPb at time t2, some batch computation involving Ra and Rb done on EPc at time t3 and results R(A,B) downloaded to EPd and EPe at time t4, see Figure -5-1.

ALTO Client themselves can schedule their requests, as they know *when* noticeable ALTO values may occur.

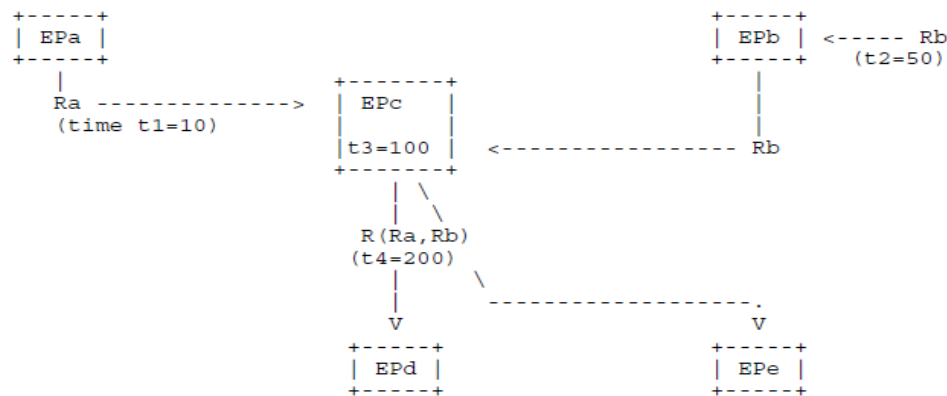


Figure -5-1: example of a UE (EPe) that performs a non real time application involving other Endpoints at different times and where these Endpoints connect w.r.t. a Cost Schedule.

5.2.1.1.3 Use case 2: Variable connectivity to a content location

A use case showing a UE that performs video download and has the choice to connect to several possible Video Caches (Endpoints) and that experiments QoE degradation e.g. due to a decrease of the path quality between the UE and the different Endpoints. This use case is very representative of the usefulness for UE in wireless networks to be able to schedule their choice on the Endpoints to connect to w.r.t. to the predicted path quality. A path quality may be predictable for instance w.r.t. busy hours or other network management policy considerations. In that case, the network operator may provide ALTO Clients with a schedule that provides time-based path costs to Endpoints. Figure 5-2 shows the proof of concept demonstrated for the the association of the ALTO protocol and IP mobility and described in Section 3.2.2. This demonstration involved the base protocol and the figure shows that four steps are needed in this case to connect to a better Endpoint upon QoE degradation.

Figure 5-3 shows a scenario on how time and QoE disturbance can be avoided with the ALTO Cost Schedule, as the UE and ALTO Client can anticipate it. In this example, QoE is not dierectly predicted but is abstracted in a routing cost, whose values are set so as to guide the UEs to connect to Endpoints according to the mutual interest of the network provider and the application consumer.

5.2.1.1.4 Achievements

- The IETF ALTO protocol extension ALTO Cost Schedule studied within the Mevico project has been specified and presented at the IETF ALTO WG, see [Randriamasy12] and [Randriamasy12-2].
- The motivating use case illustrated in Figure 5-3 and Figure 5-3 have been demonstrated at the final Mevico Review.

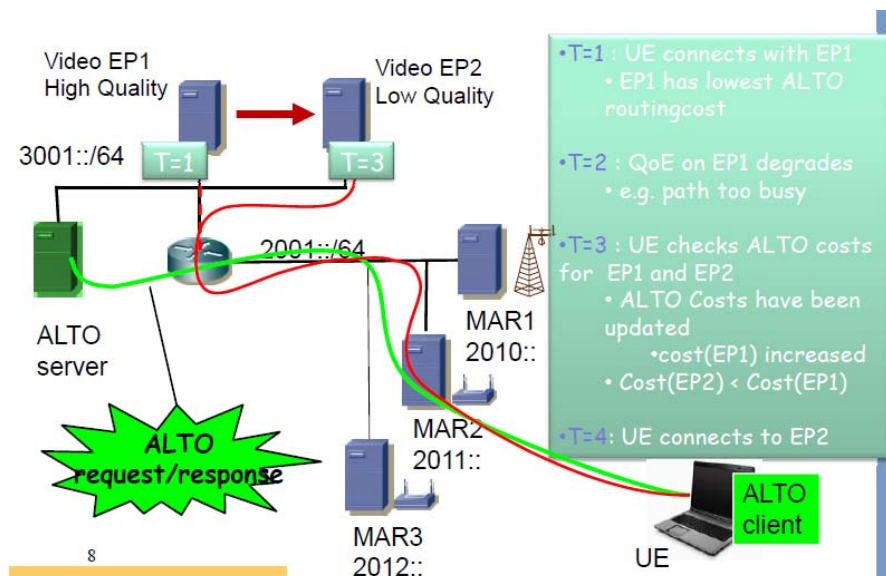


Figure 5-2 Use case 2: the UE connects to Video Server Endpoints selected with the support of the base ALTO protocol.

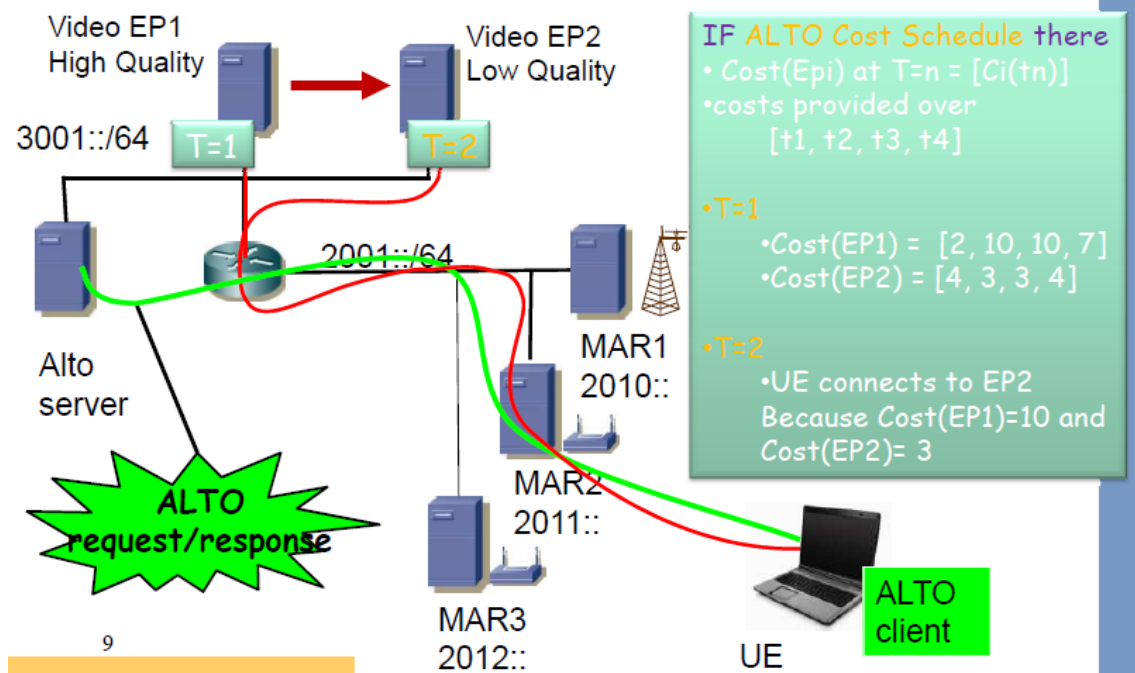


Figure 5-3: Use case 2: the UE connects to Video Server Endpoints selected with the support of the ALTO Cost Schedule

5.3 P4P

In P2P file sharing applications, the content which is interested, generally available more than one user. An P4P file sharing service using ALTO may provide information either users or applications in order to make more efficient user selection according to underlying network. ALTO protocol defines two types of map service, Network Map and Cost Map. Under these directories distributed applications can achieve topology information of the corresponding network as well as the cost values between end-points. It is important to note that, the way of forming network map and the corresponding cost map is left to the companies that implement and sell it in order to develop their innovative ideas and create a difference.

We add and analyze ALTO Service in a BitTorrent-Like P2P file sharing application. The reason why we implement a BitTorrent-Like protocol is, it is the leading P2P file sharing application, and it generates the 50% of in whole Internet traffic on the average [Xia10]. Therefore, improving the performance of this protocol with ALTO Service, also affects the operational costs of the ISPs in terms of bandwidth demand in a good way as well.

5.3.1 BitTorrent Protocol

BitTorrent is a tracker-based P2P file sharing tool which is used most of the internet users today. In BitTorrent, users not only download content from the server but also serve it to the other peers. Thus the serving capacity of the system grows with the number of nodes, making the system potentially self-scaling. The idea behind BitTorrent is to divide entire content into small pieces called chunks (typically 256 Kbyte size) and share and upload them the other users. There are two different user type defined in BitTorrent which are seed and peer. Seed is used for the nodes who has the entire content and only upload it to the requested users. Peer on the other hand is called for the user who has none or non-entire of the content. As can be understood from the definitions, seeds only upload the corresponding content like servers, and peers upload the corresponding content to requester peers and download the non-existing chunks from the other peers, simultaneously. The general working mechanism of BitTorrents is as follows;

1) First, a user in BitTorrent overlay, creates an encrypted metadata file called torrent file of the content it wants to share, with other users in the overlay and then publish it via Web. It contains no information about the content of the file. The only data that the torrent holds is, the information about the location of different pieces of the target _le. It also contains the URLs of many central, determined control servers' (called trackers) information and integrity metadata about all the pieces.

- 2) Peers who want to download the content first obtain the corresponding torrent file from Internet and run this file via the application.
- 3) Since the torrent file includes information (URL Address) about the tracker peer connects the server and request for a peer list in order to start downloading.
- 4) Once receiving this request tracker sends a randomly generated peer list that have the chunks corresponding content.
- 5) Having received the peer list response peer starts downloading the chunks from the other peers. Figure 5-4 summarizes the overall chronological progress.

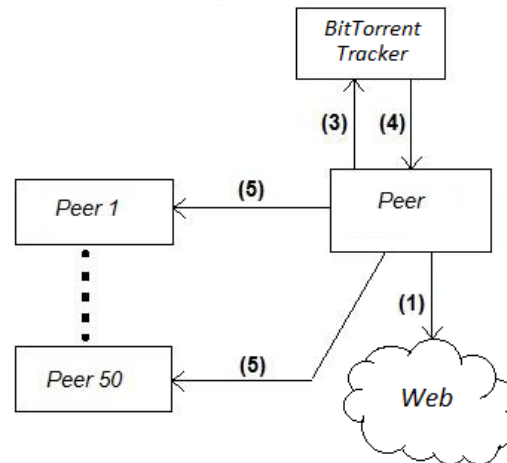


Figure 5-4: BitTorrent Mechanism

5.3.2 Proposed Network Model

We simulated two different BitTorrent-Like file sharing scenarios with and without ALTO Service, those include 780 peers, one tracker and three ALTO Servers each of them are placed to each ISP. In the first scenario, when a peer wants to the overlay, it also sends information about which chunks of the file it has or has not as well. Then, when the tracker receives the request from the corresponding peer, it registers the peer and sends a randomly created peer list that includes 20 peers' IP addresses. The peer that receives the peer list start to establish TCP connections with the peers those are in peer list. Besides, every peer in the overlay sends updated information about which chunks it has to the tracker with a 10 seconds period of time. In the second scenario, three ALTO Servers are made active in each ISP to provide Network Map and Cost Map information. Therefore, before creating and sending a peer list, tracker obtains the Cost Map information from the corresponding ALTO Server, as shown in Figure 5-5. Once getting the related cost values between peers which are calculated by using the Distance Based cost calculation method, tracker creates a ranked peer list and sends it to the requester peer for better performance. In the Minimum Distance Based cost calculation method ALTO Server does nothing but calculates the physical hop number between the requester peer and the candidate peers until reaching it and then assigns an ordered costs. As a detail, in both of the scenarios we assume that, initially all of the peers have the .torrent file which is needed to connect to the tracker. Also upload and download bandwidth rates are distributed to the peers according to Table 5-1. It is important to note that every ISP has a direct link to other two ISPs as shown in Figure 5-6. Besides, the internal physical topology of an ISP is shown in Figure 5-7, as well. In that topology model we see that, for simplicity the connections between routers are made according to tree based model all in three ISPs. In other words, in overall topology, there is only one path from any peer to any peer. Therefore, this situation lets us avoiding multiple routing path issues for this study. As a note, we are going to use the same topology with a minor change in the next study, again. The size of the content is set 16 Mbytes and the simulation is run for 6 minutes.

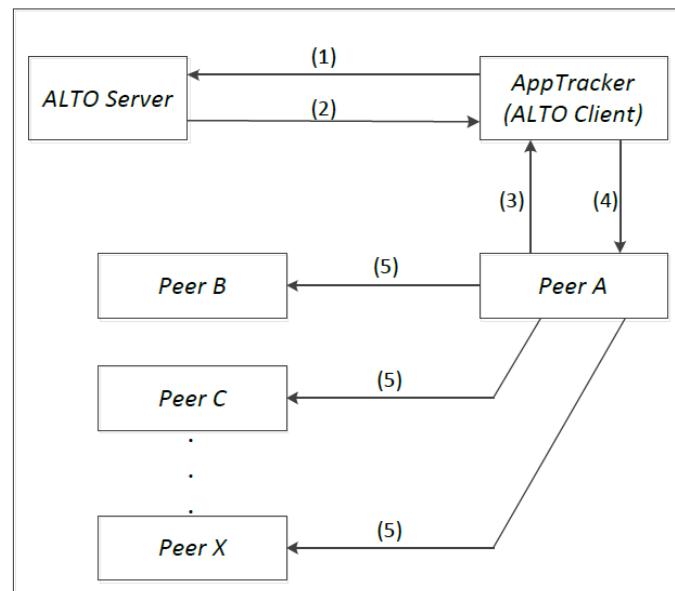


Figure 5-5: ALTO Client embedded in P2P Tracker

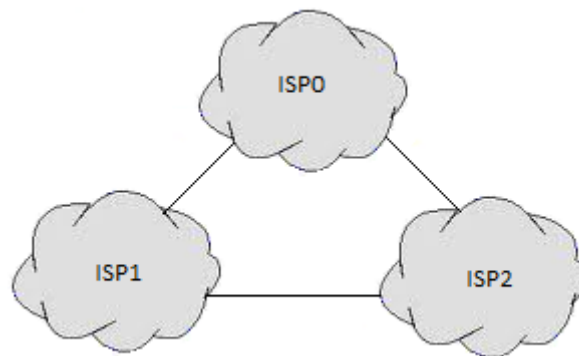


Figure 5-6: Proposed Network Model

Table 5-1 : Bandwidth Distributions of Peers

Percentage(%)	Upload Bandwidth(Mbps)	Download Bandwidth(Mbps)
56	0.5	0.25
21	3	0.4
9	1.5	0.9
3	20	2
11	20	5

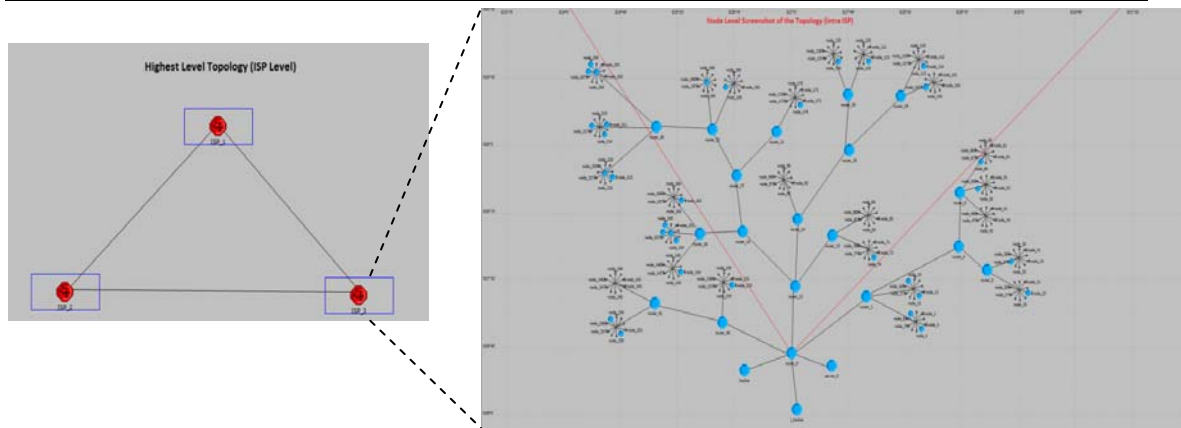


Figure 5-7: ISP Topology

5.3.3 Summary of Evaluation Results

We focus on two results, that are Inter-ISP traffic rate and content downloading completion time of the peers. Simulation results show that the average cross domain traffic rates are reduced approximately half of them by using ALTO service. Random peer selection process causes inefficient peer lists in terms of cross-domain traffic. Similarly, the results on the content downloading completion time show improvement, as well.

6 Integration of technologies

In this section each traffic management technology is discussed from the integration point of view. In the followings it is described what kind of decisions are made, how they are performed and what are the influences of the different proposals on the MEVICO TM architecture.

We believe that our work and more precisely this section about TM integration could help the R&D department of an operator or vendor to decide on what improvements to make on its existing infrastructure, existing solutions. At the end, due to the long development and integration processes, very few improvements are likely to be realized by the operator or the vendor on an existing infrastructure. Hence when discussing integration, it is more important to provide detailed information on the functions of candidate traffic management solutions in order to support the decisions of the R&D department, than make subjective guesses on possible combinations of these technologies to be integrated as a combined traffic management architecture.

Anyhow, as far as we can see, most of these technologies would not conflict when integrating them together into one architecture, because they provide quite different functionalities as presented by Figure 1. Figure 1 illustrates the logical structure of the proposed technologies. Technologies are positioned in terms of their place and influence in the network segments and layers of the MNO.

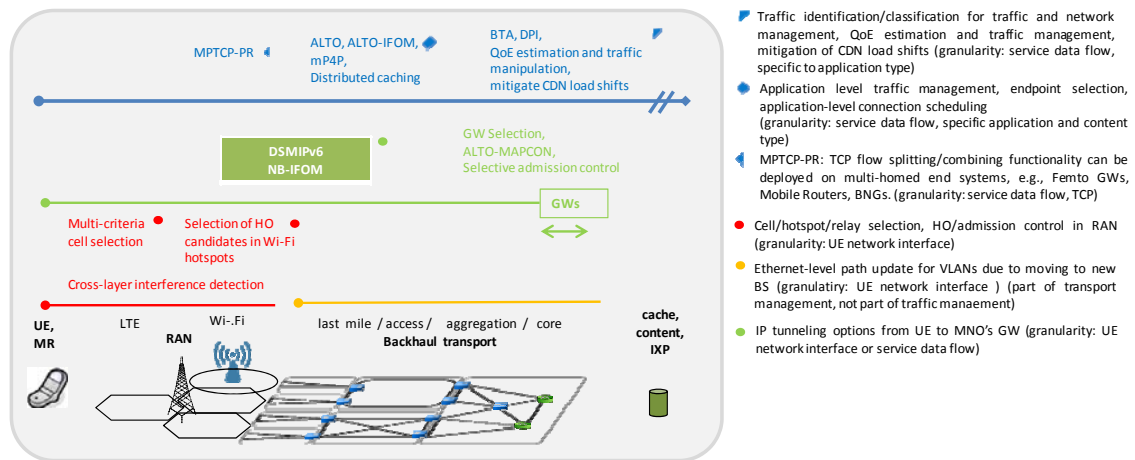





Figure 1 – Logical structure of TM technologies

The technologies can be grouped into the following categories regarding their position in the network layers and segments, and their influence on network resource utilization; RAN layer optimization, Transport layer optimization, Mobile service core optimization and application level optimization.

- **RAN layer optimization** (combined with backhaul): red technologies influence radio access network selection with user-level granularity, and include RAN-layer traffic management. These technologies determine 3GPP cell / Wi-Fi hotspot selection for the UE's network interfaces (as indicated by ●) hence optimize RAN and backhaul network resource utilization.
- **Transport-layer optimization** (on different backhaul network segments or core transport): yellow technologies improve the transport network layer's capacity, increase the transport connectivity possibilities, provide capacity improvements, fault-tolerant transport. These technologies are described in [D3.2].
- **Mobile service core optimization**: green technologies influence UE interface selection, GW selection, the path between UE/MR and GW by route optimization. These technologies assign traffic flows to a given UE network interface on IP-level. Part of them provide IP-level handover execution for the UE/MR (as indicated by ●), and are the enablers for network-controlled macroscopic traffic management. The traffic steering to new interface can be user or flow level at these technologies. Gateway selection algorithm determines the other end of the path; it works on user-level and is restricted to S-GW, P-GW selection. The optimal placement of multiple S-GW/P-GWs (as indicated by the green arrow) is influenced by many factors such as demand traffic matrix, breakout possibilities given by transport network layer and tunneling options, content location (caches, CDN). The CAPEX/OPEX analysis described in [D1.4] indicates which topology is the best to use.
- **Application-level optimization**: blue technologies are providing traffic management functionalities on application-level. The traffic treatment granularity of the technologies in this group is flow-level, they are restricted to specific transport-layer protocol or application type.

- Technologies, such as ALTO and P4P influence the endpoint selection and load scheduling for specific applications (as indicated by ) , hence they provide better spatial and temporal distribution of these traffic demands, considering network operator aspects, such as network utilization.
- It is possible to deploy MPTCP-PR (TCP flow splitting/combining functionality) on multi-homed end systems (the GWs), such as multi-homed Femto GWs, Mobile Routers, BNGs, enabling capacity aggregation for specific TCP flows going through the end-system (as indicated by ) .
- Traffic identification and classification technologies are used by traffic and network management. QoE estimation and traffic management technology identifies QoS degradations for video streams and updates the stream bandwidth and other parameters accordingly. Mitigation of CDN load shifts is a technology influencing the resource utilization of the network segments between MNO's GWs and other IXPs, accordingly (as indicated by ) .

We found that the main concern of integration from high-level design aspect is to check that the newly integrated technologies together with the existing functions will not conflict in terms of optimization goals. The symptoms of such conflicts are prohibition of each other to reach their goals, traffic fluctuations or continuous reallocation of flows to paths by TMs working on different layer and different granularities.

To enable investigation of possible conflicts with other technologies, we summarized for each technology the most relevant parameters on their decision logic, input parameters, triggers, time scale, influence on network segments, etc.

6.1 ALTO

ALTO influences the endpoint selection and load scheduling for ALTO-aware applications. It improves the spatial and temporal distribution of the traffic demands of these applications. Since ALTO server is operated by the MNO, network operator aspects, such as network utilization, can be considered.

ALTO Cost map and Endpoint costs help in the selection of Endpoint for the content. ALTO Cost schedule extension will help application to schedule their connection at time favorable wrt network usage. ALTO P4P reduces inter-domain traffic.

ALTO may have some impact on the UE on the application-level (ALTO client is necessary). On the network side ALTO server is required. It influences the path from UE to MNO-operated content server.

Technology	ALTO-IFOM (ALTO-assisted update of Connection Node (CN) upon IFOM)
Info for decision logic	ALTO is managed by operator that gives info about the path. The UE embeds an ALTO client; the ALTO client communicates with the connection manager (CM). The decision is based on the following information (working assumptions): <ul style="list-style-type: none"> - the UE embeds an ALTO client and the ALTO client communicates with the connection manager. - the UE is connected or is going to connect via IFOM or MAPCON, to CNs selected with the help of the ALTO protocol. - the UE has already collected the set of eligible CNs - the UE queries and receives the path cost to these CNs from an ALTO server, that is located so as to gather information at least on the EPS bearer between UE and PGW and on the path from PGW to each CNs not located in the EPS covered by the ALTO server
Frequency of decision	UE will request ALTO server info about the cost of the path (via HTTP request). It is on application need basis when UE request the info from ALTO server. The required time for CN update after IFOM HO \geq time needed to query and receive path cost from UE to eligible CNs from an ALTO server (HTTP request).
Info that triggers decision	trigger = IFOM HO on connections to CNs with ALTO-aware applications.
Network element that collects info for decision	ALTO server
Network element that executes decision	UE
How to enforce the decision	UE will initiate the IFOM HO based on ALTO server response. The HO is performed using DSMIPv6.

Tunneling or transport protocol used	DSMIPv6
Access scenarios supported by UE (single / multi-access)	ALTO-IFOM requires multi-access
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	All the path is influenced, except the GW in case of IFOM
Which of these parameters will this technology have influence	communication path, scheduling between GW-Endpoint or between UE-Endpoint, on application level, load distribution
Is the mechanism Microscopic/macrosopic or application related?	MacroTM granularity: fivetuple
Typical scenario where the technology is applied	CDNs, any application which uses ALTO, like P4P
Comments	Compared to NB-IFOM: this could be the first phase of the operation (select path between UE and GW)

Table 6-1: ALTO-IFOM

Technology	ALTO-MAPCON (ALTO-assisted joint selection of CNs and APNs for MAPCON capable UEs)
Info for decision logic	ALTO is managed by operator that gives info about the path. The UE embeds an ALTO client; the ALTO client communicates with the connection manager (CM). The decision is based on the following information (working assumptions): <ul style="list-style-type: none"> - the UE embeds an ALTO client and the ALTO client communicates with the connection manager. - the UE is connected or is going to connect via IFOM or MAPCON, to CNs selected with the help of the ALTO protocol. - the UE has already collected the set of eligible CNs - the UE queries and receives the path cost to these CNs from an ALTO server, that is located so as to gather information at least on the EPS bearer between UE and PGW and on the path from PGW to each CNs not located in the EPS covered by the ALTO server
Frequency of decision	UE will request ALTO server info about cost of the path (via HTTP request). It is on need basis when UE request the info from ALTO server. The time needed to select CN and associated APN \geq time needed to query and receive path cost from UE to eligible CNs from an ALTO server (HTTP request).
Info that triggers decision	trigger = Selection of CNs with ALTO with awareness of MAPCON capability. Decision making entity embedded in UE.
Network element that collects info for decision	ALTO server
Network element that executes decision	UE
How to enforce the decision	Selection of Connection Node and MAPCON capability info. The HO is performed using DSMIPv6.
Tunneling or transport protocol used	DSMIPv6
Access scenarios supported by UE (single / multi-access)	ALTO-MAPCON supports both single-access and multi-access scenarios
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	All the path is influenced
Which of these parameters will this technology have influence	communication path, scheduling between GW-Endpoint or between UE-Endpoint, on application level, load distribution
Is the mechanism Microscopic/macrosopic or application related?	MacroTM granularity: fivetuple

Typical scenario where the technology is applied	CDNs, any application which uses ALTO, like P4P
Comments	Compared to NB-IFOM: this could be the first phase of the operation (select path between UE and GW)

Table 6-2: ALTO-MAPCON

6.2 NB-IFOM

The objective is to implement different flow-level load-balancing strategies enforced by Network-based DSMIPv6. The decision and enforcement is flow-level, and the result is that flows are allocated to given UE interface, RAN and backhaul towards the HA. Consequently NB-IFOM has gains in multi-access scenarios. NB-IFOM is restricted to UEs that register to the given HA (during GW selection). Currently, without global HA-HA mobility extension, it supports only centralized mobility management.

Different load balancing strategies are implemented which specify where a flow is mapped, until there is no problem: 1) round-robin enforcing uniform distribution of SDFs among available uplinks, 2) least used enforcing the mapping of traffic to least used RAN and backhaul segment, depending current BW on UL, 3) lowest latency depending on current latency on UL, 4) overflow which waits while a link becomes full, does not utilize all accesses.

As the QoS of a flow measured by DPI or a network parameter provided by network management becomes suboptimal, policy change events are triggered, to reallocate flows to other accesses. The implementation of these policies is still future work.

Technology	NB-IFOM (Network-based IP Flow Mobility)
Info for decision logic	The decision is based on entity data such as flow id, and link or network based information such as bandwidth, packet loss, and latency.
Frequency of decision	Can vary from coarse grain (several minutes) to fine grained (couple of seconds). This might be defined by the operator or manufactured.
Info that triggers decision	Triggering information is based on real-life network monitoring and network management data.
Network element that collects info for decision	DPI and network management provides info to PCRF related to the flows, links status, etc. PCRF makes the decision based on these information and based on static rules defined by operator (e.g., subscription data). The PCRF receives changes in UEs policies through Gx interface.
Network element that executes decision	P-GW makes the decision
How to enforce the decision	DSMIPv6
Tunneling or transport protocol used	DSMIPv6
Access scenarios supported by UE (single / multi-access)	multi-access
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	RAN/backhaul/core until GW
Which of these parameters will this technology have influence	communication path between (UE interface selection is affected on flow-level), load-distribution
Is the mechanism Microscopic/macroscopic or application related?	MacroTM fivetuple
Typical scenario where the technology is applied	Multi-access environments with overlapping coverage areas
Comments	

Table 6-3: NB-IFOM

6.3 MCCS

Multi-criteria cell selection considers hierarchical 3GPP RAN cell structure. The cell selection for a given UE has influence on the 3GPP RAN throughput and radio transmission delay. The objective of the validation was the comparison of the performances of distance based cell selection, SINR based cell selection and global cell selection algorithm. Furthermore PF schedulers have been compared to RR schedulers. The validation scenario included 1 macro-, 0...2 pico-, 0...4 femtocells and 20...100 UEs. The analysis of MCCS methods was restricted to 3GPP-access networks but the topic can be extended to multi-access environments. The granularity of the traffic steering by this technology is device level (3GPP RAN network interface level).

Technology	MCCS (Multi-criteria cell selection)
Info for decision logic	Distance between UE and cells SINR Load on the BSs and the achievable average rate The average supportable rate for user j by cell i.
Frequency of decision	When a UE enters a different cell site
Info that triggers decision	Traffic load in the cell, user's quality of services, user's channel quality.
Network element that collects info for decision	UE, eNodeB and MME
Network element that executes decision	MME
How to enforce the decision	The UE gets CQI information to the candidate eNodeB. The resources in eNodeB and users CQI are sent to the MME which then makes the decision.
Tunneling or transport protocol used	all
Access scenarios supported by UE (single / multi-access)	3GPP-access but can be extended to multi-access
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	RAN
Which of these parameters will this technology have influence	load distribution in RAN, backhaul
Is the mechanism Microscopic/macrosopic or application related?	in case of single-access: all flows moved, device-level
Typical scenario where the technology is applied	any cellular network
Comments	operates in RAN, no conflict with other technologies

Table 6-4: MCCS

6.4 Selection of HO candidates in Wi-Fi hotspots

This technology focuses on decision algorithms for Wi-Fi offload, i.e., user selection in order to increase the efficiency of Wi-Fi resource utilization and maximize the offload to Wi-Fi access. It assumes operator managed Wi-Fi hotspots, or public hotspots. This network based access selection algorithm can be implemented in Wi-Fi APs or to separate network entities. The decision algorithm assumes multi-access scenario: users not connecting to Wi-Fi are assumed to access through 3GPP RAN.

Wi-Fi capacity is filled up with randomly selected terminals (as users/operator are willing to connect the user to Wi-Fi), however, when the QoS degradation of certain flow-types connecting through Wi-Fi reach some threshold value, one STA is selected and disconnected from Wi-Fi. QoS monitoring is application-aware, meanwhile the enforcement is user-level. Three selection schemes of STAs have been compared to decide which STA should be disconnected from Wi-Fi in such situation: 1) Random selection, which lowers the load in the network by randomly selecting a terminal, has very low complexity, but is RAN-layer technology-agnostic; 2) RSSI-based selection, where high received signal strength indicates good wireless channel, and accordingly we select the terminal with lowest RSSI value; 3) a novel Cost Function Approach (CFA), which selects inefficient terminals based on explicit evaluation of Wi-Fi

transmission parameters. Within CFA two approaches are considered a) one based on inefficiency metric, b) the other based on weighted aggregation of inefficiency and current network load of a STA.

Technology	Selection of HO candidates in Wi-Fi hotspots
Info for decision logic	Throughput is measured for each flow in the AP that picks out the user with worse cost metric. Cost metric can be: random selection, RSSI, Inefficiency, equal weights.
Frequency of decision	~100 ms
Info that triggers decision	violation of QoS constraints (SCTP throughput e.g.)
Network element that collects info for decision	WLAN AP (in AP or separate entity), also in the 3GPP-RAN. Signaling delay should be 10 ms. Placement is not a constraint
Network element that executes decision	WLAN AP
How to enforce the decision	vertical HO: UE-based HO could be faster than NB, but NB-IFOM could consider more information, not just Wi-Fi resource utilization
Tunneling or transport protocol used	all
Access scenarios supported by UE (single / multi-access)	multi-access scenario, two types of networks must be available
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	depends on where Wi-Fi access is connected
Which of these parameters will this technology have influence	maximize the WLAN cell utilization, goodput of users
Is the mechanism Microscopic/macrosopic or application related?	MacroTM enforcement works currently per UE, but could be extended to per flow
Typical scenario where the technology is applied	any hotspot scenario (e.g. airport)
Comments	

Table 6-5: Selection of HO candidates in Wi-Fi hotspots

6.5 GW selection

GW selection influences which GW must be selected for a given tunneling option/IP connectivity, and is not restricted to any tunneling option. Its usage is appropriate in any network architecture with multiple GWs. In 3GPP standard the following parameters influence the selection: used service class (APN), area served by S-GW, distance between S-GW and eNB (ordered list in DNS response), distance between PGW and service domain (ordered P-GW list in the DNS response), load of the GW, topological proximity of S-GW and P-GW (knowing from the structure of DNS name of the GWs). The added feature is to consider the following parameters as well: load of the transport network, access network supported by the GW and the UE. Regarding scenarios, GW selection is restricted to S-GW, P-GW selection executed by the MME. In case of IFOM, GW selection is activated before IFOM operations in order to select the GW for the lifetime of the IFOM connection. In case of MAPCON, GW selection could be used for selection of second GW as well, furthermore to decide where to assign a given flow.

Technology	GW selection
Info for decision logic	The information is collected in the S/P-GW. The measurement is done in the links. The load can be collected from the network management. Collect usage information.
Frequency of decision	Seconds or minutes. At initial attachment (MME decides), or new PDN connection establishment.

Info that triggers decision	There is a threshold that indicates the GW is being congested and no new new users get connected to the GW that is connected. The MME will decide the GW to the used when GW is overloaded. The GW can also modify DNS entry to return different GW.
Network element that collects info for decision	S/P-GW
Network element that executes decision	S/P-GW
How to enforce the decision	
Tunneling or transport protocol used	all, in case of DSMIPv6: HA address selection
Access scenarios supported by UE (single / multi-access)	all
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	In centralized cases it influences mainly which GW is loaded. In distributed or flat cases, the backhaul load might also be influenced.
Which of these parameters will this technology have influence	
Is the mechanism Microscopic/macrosopic or application related?	MacroTM: granularity per UE
Typical scenario where the technology is applied	any mobile networking architecture with GW nodes
Comments	in case of IFOM, GW selection comes into picture before IFOM operations, in order to select the GW. In case of MAPCON, GW selection may be used not only for selection of the second GW but also for where to map a given flow.

Table 6-6: GW selection

6.6 Bulk Traffic Analysis

MNOs would like to understand the usage of the network in detail. This technology provides a cost-efficient solution to get full picture on network usage. The usage will be categorized into P2P, Conversational (VoIP, IM, Video chat), Video, Web browsing. In addition to this the detailed reports will be displayed for the following application types: 1) P2P protocol type, 2) conversational: application-type like Skype, talk, 3) Video: distribution into youtube, Facebook, dailymotion, etc., 4) Web browsing: distribution of usage into URLs. This will enable a network operator to understand usage to make additional settings on PCRF, provide more efficient campaigns.

Reporting can also be done by DPI, however in order to achieve that, detailed configurations and settings are necessary in the network. This would require an immense amount of investment and operational costs would be high.

Technology	BTA
Info for decision logic	not valid
Frequency of decision	not valid
Info that triggers decision	not valid
Network element that collects info for decision	PGW
Network element that executes decision	PCRF, PCEF, and the "Campaign management system"
How to enforce the decision	PCEF
Tunneling or transport protocol used	all
Access scenarios supported by UE (single / multi-access)	all

Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	indirect impact on everything which uses the information provided by DPI or by BTA
Which of these parameters will this technology have influence	
Is the mechanism Microscopic/macrosopic or application related?	MicroTM
Typical scenario where the technology is applied	network planners can make adjustments according to reports gathered from the BTA, marketing can generate new campaigns and usage plan sizes
Comments	

Table 6-7: BTA

6.7 Deep Packet Inspection

Deep packet inspection enables to get detailed view on traffic flows and their QoS/QoE, which can be used as input for network management and traffic management. It enables policy enforcement from low to very high granularity.

Technology	DPI
Info for decision logic	not valid
Frequency of decision	not valid
Info that triggers decision	not valid
Network element that collects info for decision	PGW (itself is an information collector)
Network element that executes decision	PCRF, PCEF, and the "Campaign management system"
How to enforce the decision	PCEF
Tunneling or transport protocol used	all
Access scenarios supported by UE (single / multi-access)	all
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	indirect impact on everything which uses the information provided by DPI or by BTA
Which of these parameters will this technology have influence	
Is the mechanism Microscopic/macrosopic or application related?	MicroTM
Typical scenario where the technology is applied	#as above, but can be real-time (if it deals with specific issues which have not serious performance impacts) and more dynamic! #QoE estimation of user traffic #NB-IFOM + DPI, also used to identify flows for QoE estimation and flow manipulation
Comments	IPsec question could be investigated. It narrows down DPI monitoring to the Gi interface

Table 6-8: DPI

6.8 QoE estimation and traffic manipulation

QoE estimation has no impact on existing network elements. Similar to DPI, it doesn't increase the overall throughput or performance. It can be seen as a mechanism that can be used to evaluate other optimization techniques to improve their effectiveness with respect to the user's QoE. This technique is

particularly useful for improving overall user experience when using real-time video streaming based on, for instance, RTSP and RTP protocols.

Technology	QoE estimation and flow manipulation
Info for decision logic	
Frequency of decision	
Info that triggers decision	
Network element that collects info for decision	
Network element that executes decision	
How to enforce the decision	
Tunneling or transport protocol used	all, because it is behind the GW
Access scenarios supported by UE (single / multi-access)	any
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	the whole path, by throttling the volume of a flow
Which of these parameters will this technology have influence	
Is the mechanism Microscopic/macrosopic or application related?	MicroTM
Typical scenario where the technology is applied	
Comments	

Table 6-9: QoE estimation and traffic manipulation

6.9 MPTCP-PR

MPTCP-PR provides multipath support for TCP-based applications without implications on the UE. TCP flow splitting/combining functionality could be deployed on multi-homed end systems, Femto GWs, MRs in case of NEMO scenarios. By offloading some of the TCP traffic via breakouts, the MNO's access and backhaul network will be prevented from excessive data traffic. The granularity of this traffic management solution is under TCP flow-level.

Technology	MPTCP-PR
Info for decision logic	not valid for the current version, but a weighted scheduling could be implemented on every proxies and based measurements more packets can be sent to higher rated paths.
Frequency of decision	not valid for the current version, RTT
Info that triggers decision	perceived RTT values
Network element that collects info for decision	the proxy itself
Network element that executes decision	the proxy itself
How to enforce the decision	the proxy itself by using the defined scheduler
Tunneling or transport protocol used	all
Access scenarios supported by UE (single / multi-access)	all

Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	GWs (first user plane IP routers) to IXPs
Which of these parameters will this technology have influence	
Is the mechanism Microscopic/macrosopic or application related?	MicroTM/MacroTM
Typical scenario where the technology is applied	#for flat architectures: load distribution of backhaul and core segments #for legacy 3GPP architectures: HeNodeB GW placement is a promising application area
Comments	On the proxy MPTCP or any other congestion control protocol can be used, the solution is transparent for the actual transport

Table 6-10: MPTCP-PR

6.10 mP4P

This technology brings QoE improvements for users connecting with P2P applications, furthermore reduces the network utilization mainly on the network segment from GWs to IXPs.

The aim of the validation was to compare ALTO-server aided P4P video delivery with normal P2P video delivery using simulations. A topology with 3 ISPs in a fixed network has been used containing in total 750 peers assigned with random bandwidth, 30 seeds with 16 MB content, one AppTracker, one ALTO server for each ISP.

Technology	P4P
Info for decision logic	Based on iTracker operation considering peer ranking mechanisms
Frequency of decision	For accurate peer ranking each peer receives a new peer list every 5 seconds, but the period can be adjusted. The period should be short enough for high performance, long enough to reduce excess traffic load.
Info that triggers decision	A mobile tries to join the overlay
Network element that collects info for decision	iTracker and appTracker
Network element that executes decision	iTracker
How to enforce the decision	iTracker gives back the appropriate list of peers to the mobile
Tunneling or transport protocol used	all
Access scenarios supported by UE (single / multi-access)	all
Which part of the data path (LTE/EPC RAN/backhaul/core/GWs to ISPs) is influenced by the technology	behind the GW within the control of ISPs
Which of these parameters will this technology have influence	
Is the mechanism Microscopic/macrosopic or application related?	application
Typical scenario where the technology is applied	mobile content delivery, all the ALTO scenarios from above
Comments	Each ISP should own their iTracker (ALTO server) and operate it behind the GW

Table 6-11: mP4P

7 Conclusions

This document is the final document of the MEVICO traffic engineering architecture where the finalized research results have been described. State of the art in traffic engineering and the preliminary design for the MEVICO traffic engineering architecture were given in D 4.3.1.

A set of traffic engineering methods have been classified as macroscopic traffic management. Some topics that fall into this set are load and capacity aware adaptive routing in the backhaul and traffic offloading solutions.

Yet another set of techniques have been classified as microscopic traffic management are more involved with QoS requirements of individual applications. QoS support for external content is one of these traffic management challenges.

Improved resource selection & caching is the third main building block which has been handled within traffic engineering work.

An important area of work is seen as merging suggested technologies, considering the possibilities of using them together.

It can be seen that most of the technologies provide distinct functionalities and improvements in distinct areas (different scenarios, network layers). It means that their integration into a coherent architecture is possible without significant additional survey or work. However, in some special cases four of the proposed technologies (GW selection, NB-IFOM, MCCS, ALTO-MAPCON) could be subjects of further clarifications in order to prevent likely operational anomalies. These possible negative outcomes (like ping-pong effects in traffic steering) can be caused by interferences of the decision logics.

An example for such problems is when the Global Cell Selection algorithm of MCCS, NB-IFOM, ALTO-MAPCON and GW selection aim the optimization of load distribution in the backhaul segment. GW selection is not a reactive technology; it impacts network segments close to the GW nodes and avoids overloaded network states by load balancing. On the other hand, MCCS and NB-IFOM are reactive solutions. The Global Cell Selection algorithm of MCCS tries to solve backhaul congestion problems near the cells, last mile. NB-IFOM impacts the whole path between the UE and the GW as it modifies traffic distribution between available radio accesses. As a further alternative, ALTO-MAPCON offers toolset to modify the overall data path between the UE and the communication endpoint. It also should be considered whether the applied transport network layer solutions enable enough degree of freedom to remap traffic flows from the congested parts of the network. (Note that if MCCS considers only RAN optimization, then it will not conflict with the other above mentioned technologies.)

This is a complex problem without a generic solution where details of actual topologies, network parameters, operator-specific demands and precise list of feature needs from the available TM toolset are required. However, a possible approach to solve this issue could be the interlocking/prioritization/centralization of the distinct decision engines and execution/policy management schemes.

Such wide area of research needs further study for research, however individually the achieved results are quite satisfactory and will be valuable for the LTE standardization in Europe.

Acknowledgement

The work has been carried out in the framework of the CELTIC project MEVICO. The views expressed in this document are solely those of the authors and do not represent the views of their employers.

Our thanks go to all colleagues in the CELTIC project MEVICO, who have contributed to relevant documents in the project.

References

- [3GPP_29.303] 3GPP TS 29.303 V10.2.1, Technical Specification, “Domain Name System Procedures, Stage 3”, Release 10, July 2011.
- [3GPP_TR_22.805] 3GPP TR 22.805 V12.0.1: “Feasibility Study on User Plane Congestion Management”, Release 12, Sept. 2012.
- [3GPP_TR_23.829] 3GPP TR 23.829: Local IP Access and Selected IP Traffic Offload, Release 10, V1.3.0, Sept. 2010.
- [3GPP_TR_23.830] 3GPP TR 23.830 V9.0.0: “Architecture aspects of Home NodeB and Home eNodeB”, Release 9, Sept. 2009.
- [3GPP_TR_23.861] 3GPP TR 23.861 V1.3.0: “Multi access PDN connectivity and IP flow mobility”, Release 9, , February 2010.
- [3GPP_TR_23.882] 3GPP TR 23.882 V8.0.0: “3GPP System Architecture Evolution: Report on Technical Options and Conclusions”, Release 8, Sept. 2008.
- [3GPP_TR_23.8yz_UPCON] 3GPP TR 23.8yz UPCON (yz number not yet assigned) V0.1.0: “System Enhancements for User Plane Congestion Management”, Release 12, Nov. 2012.
- [3GPP_TR_23.919] 3GPP TR 23.919 V10.0.0, Technical Report, “Direct tunnel deployment guideline”, March, 2011.
- [3GPP_TR_23.919] 3GPP TR 23.919: Direct Tunnel Deployment Guideline, Release 7, V1.0.0, May 2007.
- [3GPP_TS_22.220] 3GPP TS 22.220 V10.7.0, “Service requirements for Home Node B (HNB) and Home eNode B (HeNB)”, Release 10, June 2011.
- [3GPP_TS_23.002] 3GPP TS 23.002: “Network architecture”, V12.0.0, Release 12, Sept. 2012.
- [3GPP_TS_23.060] 3GPP TS 23.060 V11.3.0, “General Packet Radio Service (GPRS); Service description”, Stage 2, Release 11, Sept. 2012.
- [3GPP_TS_23.203] 3GPP TS 23.203 V11.3.0: “Policy Control and Charging architecture”, Release 11, Sept. 2012.
- [3GPP_TS_23.216] 3GPP TS 23.216 V11.6.0: “Single Radio Voice Call Continuity (SRVCC)”, Release 11, Sept. 2012.
- [3GPP_TS_23.218] 3GPP TS 23.218 V11.4.0: “IP Multimedia (IM) Session Handling; IM call model”, Release 11, Sept. 2012.
- [3GPP_TS_23.228] 3GPP TS 23.228 V11.6.0: “IP multimedia subsystem; Stage 2”, Release 11, Sept. 2012.
- [3GPP_TS_23.234] 3GPP TS 23.234 V11.0.0: “3GPP system to Wireless Local Area Network (WLAN) interworking; System description”, Release 11, Sept. 2012.
- [3GPP_TS_23.237] 3GPP TS 23.237 V11.5.0: “IP Multimedia Subsystem (IMS) Service Continuity”, Release 11, June 2012.
- [3GPP_TS_23.261] 3GPP TS 23.261 V11.0.0, “IP flow mobility and seamless Wireless Local Area Network (WLAN) offload, Stage 2”, Release 11, Sept. 2012.
- [3GPP_TS_23.272] 3GPP TS 23.272 V11.2.0: “Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2”, Release 11, Sept. 2012.
- [3GPP_TS_23.292] 3GPP TS 23.292 V11.6.0: “IP Multimedia Subsystem (IMS) Centralized Services; Stage 2”, Release 11, Sept. 2012.
- [3GPP_TS_23.327] 3GPP TS 23.327 V11.0.0: “Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems”, Release 11, Sept. 2012.
- [3GPP_TS_23.401] 3GPP TS 23.401 V11.3.0: “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access”, Release 11, Sept. 2012.
- [3GPP_TS_23.402] 3GPP TS 23.402 V11.4.0, “Architecture enhancements for non-3GPP accesses”, Release 11, Sept. 2012.
- [3GPP_TS_24.229] 3GPP TS 24.229 V11.5.0: “IP Multimedia Call Control Protocol based on SIP and SDP”, Release 11, Sept. 2012.
- [3GPP_TS_24.301] 3GPP TS 24.301 V11.4.0: “Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)”, Release 11, Sept. 2012.

- [3GPP_TS_24.302] 3GPP TS 24.302 V11.4.0: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks", Release 11, Sept. 2012.
- [3GPP_TS_25.304] 3GPP TS 25.304 (release 8), "User equipment procedures in idle mode and procedures for cell reselection in connected mode," *Technical Specification*, 2009.
- [3GPP_TS_29.212] 3GPP TS 29.212 V11.6.0: "Policy and Charging Control; Reference Points", Release 11, Sept. 2012.
- [3GPP_TS_29.213] 3GPP TS 29.213 V11.4.0: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping", Release 11, Sept. 2012.
- [3GPP_TS_29.214] 3GPP TS 29.214 V11.6.0: "Policy and Charging Control over Rx reference point", Release 11, Sept. 2012.
- [3GPP_TS_29.215] 3GPP TS 29.215 V11.6.0: "Policy and Charging Control (PCC) over S9 reference point; Stage 3", Release 11, Sept. 2012.
- [3GPP_TS_36.300] 3GPP TS 36.300 V11.0.0: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description", Release 11, Sept. 2012.
- [3GPP_TR_36.814] 3GPP TR 36.814 (v9.0.0), "Further advancements for e-utra physical layer aspects," *Technical Specification*, 2010.
- [3GPP_TR_36.913] 3GPP TR 36.913 (v10.0.0), "Requirements for further advancements for evolved universal terrestrial radio access (eutra)," *Technical Specification*, 2011.
- [3GPP_TR_23.844] 3GPP TR 23.844 "Feasibility Study on IMS Based Peer-to-Peer Content Distribution Services; Stage 2 (Release 11)"
- [Abusubaih08] M. Abusubaih, B.Rathke, and A.Wolisz, "Collaborative Setting of RTS/CTS in Multi-Rate Multi-BSS IEEE 802.11 Wireless LANs", In Proc. of the 16'th IEEE Workshop on Local and Metropolitan Area Networks, IEEE LANMAN'08, Cluj-Napoca, Romania, September 2008
- [Abusubaih08a] M. Abusubaih and A. Wolisz, "Interference-Aware Decentralized Access Point Selection Policy for Multi-Rate IEEE 802.11 Wireless LANs", In Proc. of the 19'th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008., Cannes, France, September 2008
- [Abusubaih09] M. Abusubaih, B. Rathke, and A.Wolisz, "A framework for Interference Mitigation in Multi-BSS 802.11 Wireless LANs", In Proc. of 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2009), Kos, Greece, June 2009
- [AJZ10] V. K. Adhikari, S. Jain, and Z.-L. Zhang, "YouTube Traffic Dynamics and Its Interplay with a Tier-1 ISP: An ISP Perspective," IMC '10: Proceedings of the 10th annual conference on Internet measurement, 2010.
- [AKAM10] Akamai, State of the Internet, Quarterly Report Series (2011) <www.akamai.com>
- [ALI11] "ALTO Protocol", R. Alimi et al., June 27th 2011, <http://tools.ietf.org/html/draft-ietf-alto-protocol-09>
- [Allman09] M. Allman, V. Paxson, and E. Blanton, "TCP Congestion Control," RFC 5681, September 2009.
- [Almeida_99] S. Almeida, J. Queijo, L.M. Correia: "Spatial and temporal traffic distribution models for GSM", Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS 50th, Vol. 1., pp. 131-135
- [ALR+08] H. A. Alzoubi, S. Lee, M. Rabinovich, O. Spatscheck, J. E. van der Merwe "Anycast CDNS revisited" WWW 2008 / Refereed Track: Performance and Scalability April 21-25, 2008. Beijing, China, pp277-286
- [Al-Sanabani08] M. Al-Sanabani & al., "Mobility Prediction Based Resource Reservation for Handoff in Multimedia Wireless Cellular Networks", the International Arab Journal of Information Technology, Vol. 5, N°2, April 2008.
- [Amzallag08] D. Amzallag et al., "Cell selection in 4G cellular networks," in Proc. *IEEE Conference on Computer Communications* 2008, pp. 700-708, Apr. 2008.
- [Anpalagan99] A.S. Anpalagan and I. Katzela, "Overlaid Cellular System Design with Cell Selection Criteria for Mobile Wireless Users", *IEEE Canadian Conf. on Electrical and Computer Eng.*, vol. 1, 1999, pp. 24-28.
- [APA] Apache web server module "mod_rewrite"
http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html
- [ASK+10] B. Ager, F. Schneider, J. Kim and A. Feldmann, Revisiting cacheability in times of user generated content, Proceedings of the 13th IEEE Global Internet Symposium, San Diego, CA, USA (2010)

- [Ayar12a] T. Ayar, B. Rathke, Ł. Budzisz, and A. Wolisz, "A Splitter/Combiner Architecture for TCP over Multiple Paths", TKN Technical Report Series TKN-12-001, February 2012, available at: http://www.tkn.tu-berlin.de/menue/publications/tnk_technical_report_series/.
- [Ayar12b] T. Ayar, B. Rathke, Ł. Budzisz, and A. Wolisz, "A Transparent Performance Enhancing Proxy Architecture To Enable TCP over Multiple Paths for Single-Homed Hosts," IETF Internet Draft, draft-ayar-transparent-sca-proxy-00, Work in Progress, February 2012.
- [Ayar12c] T. Ayar, B. Rathke, Ł. Budzisz, and A. Wolisz, "TCP over Multiple Paths Revisited: Towards Transparent Proxy Solutions," In Proc. of the IEEE International Conference on Communications 2012 (IEEE ICC'12), pp. 109-114, June 2012.
- [BDK+10] L. Braun, A. Didebulidze, N. Kammenhuber, and G. Carle, "Comparing and improving current packet capturing solutions based on commodity hardware," IMC '10: Proceedings of the 10th annual conference on Internet measurement, Nov. 2010.
- [BGW10] S. Borst, V. Gupta and A. Walid, Distributed caching algorithms for content distribution networks, IEEE Infocom (2010).
- [BMV10] A. Balasubramanian, R. Mahajan, and A. Venkataramani, "Augmenting mobile 3G using WiFi," in *Proc. of MobiSys*. ACM, 2010, pp. 209–222.
- [BKC+12] "Analyzing Caching Benefits for YouTube Traffic in Edge Networks - A Measurement-Based Evaluation" L. Braun, A. Klein, G. Carle, H. Reiser, J. Eisl; NOMS 2012 IEEE Network Operations and Management Symposium Maui Hawaii USA Apr. 16th-20th 2012]
- [BPV08] R. Buyya, M. Pathan and A. Vakali (Eds.), Content delivery networks, Lecture Notes in Electrical Engineering 9, Springer (2008)
- [BRE+99] L. Breslau et al., Web caching and Zipf-like distributions: Evidence and implications, Proc. IEEE Infocom (1999)
- [CFE+06] K. Cho, K. Fukuda, H. Esaki, A. Kato, The impact and implications of the growth in residential user-to-user traffic, ACM Sigcomm Conf., Pisa (2006)
<www.acm.org/sigs/sigcomm/sigcomm2006>
- [CFM09] R. Canonico, C. Fuerer and A. Mauthe (Eds.), Content distribution infrastructures for community networks, Computer Networks Special Issue Vol. 53/4 (2009) 431-568
- [CHA+07] M. Cha et al., I tube, you tube, everybody tubes: Analyzing the world's largest user generated content video system, Internet measurement conference IMC'07, San Diego, USA (2007)
- [Cha08] B. Cha, S. Seo, Y. Choi, and J. Song, "Mobile-Velocity adaptive Vertical Handoff in Integrated WLAN and WiBro Networks," *ICIAFS 2008*, pp. 384-389. [CHA10] J. Charzinski, Traffic properties, client side cachability and CDN usage of popular web sites, Proc. 15th MMB conference, Essen, Germany, Springer LNCS 5987 (2010) 182-194
- [Chandrasekhar_08] V. Chandrasekhar, J. G. Andrews, A. Gatherer: Femtocell Networks: A Survey, IEEE Communications Magazine, 46 (9), pp. 59-67, Sept. 2008.
- [Chang10] C.-J. Chang, C.-Y. Hsieh and Y.-H. Chen, "A Preference Value-Based Cell Selection Scheme in Heterogeneous Wireless Networks," *IEEE WCNC*, 2010, pp. 1–6.
- [Chebrolu05] K. Chebrolu, B. Raman, and R. R. Rao, "A Network Layer Approach to Enable TCP over Multiple Interfaces", ACM/Kluwer Journal of Wireless networks (WINET), Vol. 11, No. 5, pp. 637-650, September 2005.
- [Chen_08] C. Chen, Y. Xu, L. Zhang: "Some Remarks on ON/OFF Network Traffic", Power Electronics and Intelligent Transportation System (PEITS), 4-5 August 2008, Guangzhou, China, pp. 515-519
- [Cheng03] P.F. Cheng and S.C. Liew, "TCP Veno: TCP enhancement for transmission over wireless access networks", IEEE Selected Areas in Communications, vol. 21, February 2003.
- [Chung02] Y. Chung, D.-J. Lee, D.-H. Cho, and B.-C. Shin, "Macrocell/Microcell Selection Schemes Based on a New Velocity Estimation in Multitier Cellular System," IEEE Trans. Vehicular Technology, vol. 51, no. 5, pp. 893-903, Sept. 2002.
- [CIS10] Cisco Systems, Visual networking index, forecast and methodology, White paper series (2011) <www.cisco.com>
- [CIS11] —, "The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular", White paper series (2011) <www.cisco.com>
- [CIU10] D. Ciullo, Network awareness of P2P live streaming applications: A measurement study, IEEE Trans. on Multimedia 12 (2010) 54-63

- [CKR+07] M. Cha, H. Kwak, P. Rodriguez, Y.-Y. Ahn, and S. Moon, "I Tube, You Tube, Everybody Tubes: Analyzing the World's Largest User Generated Content Video System," in Proceedings of the 7th Conference on Internet Measurements (IMC) 2007, 2007.
- [CKR+09] M. Cha, H. Kwak, P. Rodriguez, Y.-Y. Ahn, and S. Moon, "Analyzing the Video Popularity Characteristics of large-scale User Generated Content Systems," *IEEE/ACM Transactions on Networking (TON)*, vol. 17, no. 5, pp. 1357–1370, Oct. 2009.
- [CPZ11] "ALTO in Mobile and Wireless Network" W. Chen, J. Peng, Y. Zhang, China Mobile, July 3 2011, <http://tools.ietf.org/html/draft-chen-alto-in-mobile-wireless-network-00>
- [CSM10] G. Chatzopoulou, C. Sheng, and M. Faloutsos, "A First Step Towards Understanding Popularity in YouTube," in *INFOCOM IEEE Conference on Computer Communications Workshops*, 2010, 2010, pp. 1–6.
- [D1.2] Ivan Froger, Didier Becam (ed.) Architecture Design Release 2 Documentation, MEVICO Project Deliverable, 21. December 2011.
- [D. Y. Cl_10] D. Y. Cl.: "RF IC design of highly-efficient broadband polar transmitters for WiMAX and 3GPP LTE applications", *IEEE Solid-State and Integrated Circuit Technology (ICSICT)*, 1-4 November 2010, Shanghai, China, pp. 150-153
- [Das04] A. Das, K. Balachandran, F. Khan, A. Sampath, and H.-J. Su, "Network Controlled Cell Selection for the High Speed Downlink Packet Access in UMTS," in *Proc. IEEE WCNC*, vol. 4, pp 1975-1979, Mar. 2004.
- [DDNS] Dynamic DNS - http://www.webopedia.com/TERM/D/dynamic_DNS.html
- [DER10] L. Deri, "High Speed Network Traffic Analysis with Commodity Multi-Core Systems," *IMC '10: Proceedings of the 10th annual conference on Internet measurement*, Nov. 2010.
- [DevoTeam] DevoTeam. Traffic Load Generator. [Online]
http://www.devoteam.co.uk/index.php?option=com_content&task=view&id=445&pays=uk&Itemid=744&lang=2.
- [DVB09] Digital Video Broadcasting Project (DVB), Internet TV Content Delivery study mission report, DVB Document A 145 (2009)
<www.dvb.org/technology/standards/A145_Internet_TV_Content_Delivery_Study.pdf>
- [E_Oh_11] E. Oh et al.: "Toward Dynamic Energy-Efficient Operation of Cellular Network Infrastructure", *IEEE Communications Magazine*, June 2011, pp 56-61
- [Eck10] M. Eckert, „Analyse und automatisierte Konfiguration klassenbasierter Paketvermittlung“, 2010
- [Eck12] M. Eckert, T.M. Knoll, "ISAAR (Internet Service quality Assessment and Automatic Reaction)", Monami 2012
- [ETSI_96] ETSI GTS GSM 03.02-v5.1.0: Digital cellular telecommunications system (Phase 2+) - Network architecture (GSM 03.02), 1996.
- [EUB08] M. Eubanks, The video tsunami: Internet television, IPTV and the coming wave of video on the Internet, Plenary talk, 71. IETF meeting (2008) <www.ietf.org/proceedings/08mar/slides/plenaryt-3.pdf>
- [Evensen09] K. Evensen, D. Kaspar, P. Engelstad, A. F. Hansen, C. Griwodz, and P. Halvorsen, "A Network-Layer Proxy for Bandwidth Aggregation and Reduction of IP Packet Reordering," *IEEE 34th Conference on Local Computer Networks (LCN 2009)*, pp. 585-592, 20-23 October 2009.
- [FBA11] F. Figueiredo, F. Benevenuto, and J. M. Almeida, "The Tube over Time: Characterizing Popularity Growth of Youtube Videos," in *In Proceedings of the 4th ACM Conference on Web Search and Data Mining*, 2011.
- [FemtoForum_10] FemtoForum: Femtocells – Natural Solution for Offload – a Femto Forum topic brief, June 2010.
- [FIE00] R. Fielding et al., Hypertext transfer protocol - HTTP/1.1, Request for Comments 2616 <www.rfc-editor.org/rfc/rfc2616.txt> (2000)
- [FIE10] R. Fielding et al., HTTP/1.1, part 6: Caching, Internet-Draft
<<https://datatracker.ietf.org/doc/draft-ietf-httpbis-p6-cache/>> (2010)
- [Fiedler_Hoßfeld_Tran-Gia_10] M. Fiedler, T. Hoßfeld, P. Tran-Gia: A Generic Quantitative Relationship between Quality of Experience and Quality of Service. *IEEE Network*, Special Issue on Improving QoE for Network Services, Vol. 24 Issue 2, March-April 2010.
- [Fiercewireless_10] <http://www.fiercewireless.com/europe/story/femtocell-deployment-update/2010-09-17>
- [FMM+11] A. Finamore, M. Mellia, M. Munafo, R. Torres, and S. Rao, "YouTube Everywhere: Impact of Device and Infrastructure Synergies on User Experience," Technical Report, 2011.

- [Fodor04] G. Fodor, A. Furuskar, and J. Lundsjo. On access selection techniques in always best connected networks. In *ITC Specialist Seminar on Performance Evaluation of Wireless and Mobile Systems*, August 2004.
- [Ford11] A. Ford, C. Raiciu, S. Barre, and J. Iyengar, "Architectural Guidelines for Multipath TCP Development," RFC 6182, March 2011.
- [Ford12] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses," IETF Internet Draft, draft-ietf-mptcp-multiaddressed-07, Work in Progress, March 2012.
- [Fussen05] M. Fussen, R. Wattenhofer, and A. Zollinger, "Interference arises at the receiver", In Proc. of Wireless Networks, Communications and Mobile Computing, 2005
- [GAL+07] P. Gill, M. Arlitt, Z. Li and A. Mahanti, YouTube traffic characterization: A view from the edge, Internet measurement conference IMC'07, San Diego, USA (2007)
- [GAM07] P. Gill, M. Arlitt, Z. Li, and A. Mahanti, "Youtube traffic characterization: a view from the edge," in IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. ACM Request Permissions, Oct. 2007.
- [Gao11] L. Gao, X. Wang, G. Sun, Y. Xu, "A Game Approach for Cell Selection and Resource Allocation in Heterogeneous Wireless Networks," in Proc. of *IEEE SECON 2011*, Salt Lake City, Utah, USA, 2011.
- [Gazis05] V. Gazis, N. Alonistioti, and L. Merakos. Toward a generic "always best connected" capability in integrated WLAN/UMTS cellular mobile networks (and beyond). *Wireless Communications, IEEE*, 12(3):20–29, June 2005.
- [Gerla01] M. Gerla, M.Y. Sanadidi, W. Ren; A. Zanella, C. Casetti and S. Mascolo, "TCP Westwood: congestion window control using bandwidth estimation", in proc. of Global Telecommunications Conference, 2001 (GLOBECOM '01), 2001
- [GHAHA] R. Wakikawa, R. Kuntz, Z. Zhu, L. Zhang, Global HA to HA Protocol Specification, IETF Internet Draft, draft-wakikawa-mext-global-haha-spec-02, September, 2011.
- [GO00] G. Barish and K. Obrazcka, World wide web caching: Trends and techniques, IEEE Communications Magazine (May 2000) 178-185
- [Gomes09] J. S. Gomes, "A Rule based Co-operative Approach for Cell Selection in High Speed Cellular Networks", *IEEE International Symposium on Network Computing and Applications*, pp.74-81, 2009.
- [Guo06] Q. Guo, X H Xu, J Zhu, et al. "A QoS-guaranteed cell selection strategy for heterogeneous cellular systems". ETRI Journal, 2006, 28(1): 77–83.
- [GUO07] L. Guo et al., Does Internet media traffic really follow Zipf-like distributions? ACM SIGMETRICS (2007)
- [Hanly95] S. V. Hanly, "An algorithm for combined cell-site selection and power control to maximize cellular spread spectrum capacity," IEEE Journal on Selected Areas in Communications, vol. 13, no. 7, pp. 1332–1340, 1995.
- [Hannes] H. Ekstrom, *QoS Control in the 3GPP Evolved Packet System*, IEEE Communications Magazine (2009) 76-83
- [HAS05] G. Haßlinger, ISP platforms under a heavy peer-to-peer workload, Proc. Peer-to-Peer Systems and Applications, Eds.: R. Steinmetz and K. Wehrle, Springer LNCS 3485 (2005) 369-382
- [Haßlinger05] G. Haßlinger, S. Schnitter and M. Franzke, The efficiency of traffic engineering with regard to failure resilience, Telecommunication Systems Vol. 29/2, Springer (2005) 109-130.
- [Haßlinger11] G. Haßlinger, G. Nunzi, C. Meirosu, C. Fan and F.-U. Andersen, Traffic engineering supported by inherent network management: Analysis of resource efficiency and cost saving potential, Internat. Journal on Network Management (IJNM), Special Issue on Economic Traffic Mgmt., Vol. 21 (2011) 45-64.
- [HH10] G. Haßlinger and O. Hohlfeld, Efficiency of caches for content distribution on the Internet, Proc. 22. Internat. Teletraffic Congress, Amsterdam, The Netherlands (2010)
- [HHB09] G. Haßlinger, F. Hartleb and T. Beckhaus, User access to popular data on the Internet and approaches for IP traffic flow optimization, Proc. ASMTA Conf., Madrid, Spain, Springer LNCS 5513 (2009) 42-55
- [HMG+07] G. Haßlinger, J. Mende, R. Geib, T. Beckhaus and F. Hartleb, Measurement and characteristics of aggregated traffic in broadband access networks, Proc. 20. Internat. Teletraffic Congress, Ottawa, Canada, Springer, LNCS 4516 (2007) 998-1010

- [Holma_07] H. Holma, A. Toskala, K. Ranta-aho, J. Pirskanen: High-Speed Packet Access Evolution in 3GPP Release 7, IEEE Communications Magazine, 45 (12), pp. 29-36, Dec. 2007.
- [Hoßfeld_ Schatz_ Biedermann_11] T. Hoßfeld, R. Schatz, S. Biedermann, A. Platzer, S. Egger, M. Fiedler: The Memory Effect and Its Implications on Web QoE Modeling. Proc. ITC 2011, San Francisco, USA, September 2011
- [Hsieh05] H.-Y. Hsieh and R. Sivakumar, "A Transport Layer Approach for Achieving Aggregate Bandwidths on Multihomed Mobile Hosts," ACM/Springer Wireless Networks Journal, Volume 11, Number 1-2, pp. 99-114, January 2005.
- [HST+09] Hoßfeld, Tobias, Schlosser, Daniel, Tutschku, Kurt, Tran-Gia, Phuoc. Cooperation Strategies for P2P Content Distribution in Cellular Mobile Networks: Considering Selfishness and Heterogeneity In: Mobile Peer-to-Peer Computing for Next Generation Distributed Environments: Advancing Conceptual and Algorithmic Applications. Editor: B.-C. Seet. IGI Global, Hershey, PA, USA, May, 2009
- [HWL+08] C. Huang, A. Wang, J. Li, K. Ross, Understanding hybrid CDN-P2P, Proc. NOSSDAV Conf., Braunschweig, Germany (2008) 75-80
- [ICT_ EARTH_11] Project INFSO-ICT-247733 EARTH (EU FP7), WP2, Deliverable 2.2: "Definition and Parameterization of Reference Systems and Scenarios", June 30, 2011, pp 28-40
- [IEEE802.15.3] Draft Standard for Telecommunications and Information Exchange Between Systems -- LAN/MAN Specific Requirements -- Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN) Replaced by IEEE 802.15.3-2003, 2007
- [IEEE802.16-2004] Draft IEEE Standard for Local and metropolitan area networks Corrigendum to IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems Corrigendum to IEEE Std 802.16-2004, 2004
- [Informa_08] Informa Telecoms & Media: Mobile Broadband Access at Home – Aug. 2008.
- [IRTF] Internet Engineering Task Force (IETF) <www.ietf.org>, Internet Research Task Force (IRTF) <irtf.org>,
 - working group on Application Layer Traffic Optimization (ALTO) <tools.ietf.org/wg/alto/charters>,
 - working group on MultiProtocol Label Switching (MPLS), <tools.ietf.org/wg/mpls/charters>,
 - working group on Peer-to-Peer Streaming Protocol (PPSP) <tools.ietf.org/wg/ppsp/charters>,
 - working group on CDN interconnection (CDNI) <tools.ietf.org/wg/cdni/charters>,
 - peer-to-peer research group <www.irtf.org/charter?gtype=rg&group=p2prg>
- [ITU] International Telecommunication Union (ITU) <www.itu.int>
- [Joel_72] A. E. Joel, "Mobile Communication System," U.S. Patent 3,663,762 (May 1972)
- [KAM10] N. Kamiyama et al., ISP-operated CDN, 14th NETWORKS Telecom. Network Strategy & Planning Symposium, Warszawa, Poland (2010).
- [Karrer05] R. Karrer and E. Knightly, "TCP-PARIS: A Parallel Download Protocol for Replicas," In Proceedings of IEEE International Workshop on Web Content Caching and Distribution (WCW 2005), Sophia Antipolis, France, pp. 15-25, September 12-13 2005.
- [Kashihara10] S. Kashihara and M. Tsurusawa, "Dynamic bandwidth management system using IP flow analysis for the QoS-assured network", In Proc. of the IEEE GLOBECOM 2010, December 2010.
- [KBB10] G. Kandavanam, D. Botvich and S. Balasubramaniam, PaCRA: A path-aware content replication approach to support QoS guaranteed video on demand service in metropolitan IPTV networks, IEEE/IFIP Network Operations & Mgmt. Symp. NOMS (2010) 591-598
- [Khandekar_10] A. Khandekar, N. Bhushan, Ji Tingfang, V. Vanghi: LTE-Advanced: Heterogeneous Networks, In Proceedings of the European Wireless Conference, pp. 978 – 982, April 2010.
- [Kim07] K.-H. Kim and K. G. Shin, "PRISM: Improving the Performance of Inverse-Multiplexed TCP in Wireless Networks," IEEE Transactions on Mobile Computing, Vol. 6, Issue 12, pp. 1297-1312, December 2007.
- [Kim09] S.-W. Kim, Y.-H. Lee, "Adaptive MIMO Mode and Fast Cell Selection with Interference Avoidance in Multi-cell Environments," 5th International Conference on Wireless and Mobile Communications (ICWMC), pp.163-167, 2009.
- [Kineto10] Kineto Wireless, "Smart Offload for Smartphones," Whitepaper, 2010.
- [Klein04] T. Klein et al., "Assignment strategies for mobile data users in hierarchical overlay networks: performance of optimal and adaptive strategies," IEEE J. Sel. Areas Commun., vol. 22, no. 5, June 2004.

- [Knoll12] Knoll T. M.: Cross-Domain and Cross-Layer Coarse Grained Quality of Service Support in IP-based Networks; <http://archiv.tu-chemnitz.de/pub/2009/0165/>
- [Kostopoulos10] A. Kostopoulos, H. Warma, T. Leva, B. Heinrich, A. Ford, and L. Eggert, "Towards Multipath TCP Adoption: Challenges and Opportunities," 6th EURO-NF Conference on Next Generation Internet (NGI), pp. 1-8, Paris, 2-4 June 2010.
- [Kwan_Cong_10] R. Kwan, R. Arnott et al., "On Pre-emption and Congestion Control for LTE Systems", Proc. of IEEE Vehicular Technology Conference (VTC), Fall, 2010
- [Kwan_Mob_10] R. Kwan, R. Arnott et al.: "On Mobility Load Balancing for LTE Systems", Vehicular Technology Conference Fall (VTC 2010-Fall), 2010
- [Kwan_Radio_10] R. Kwan, R. Arnott et al., "On Radio Admission Control for LTE Systems", Proc. of IEEE Vehicular Technology Conference (VTC), Fall, 2010
- [Kwon11] Y. J. Kwon, D.-H. Cho, "Load Based Cell Selection Algorithm for Faulted Handover in Indoor Femtocell Network", *IEEE VTC Spring*, pp.1-5, 2011.
- [Lagrange96] X. Lagrange, P. Godlewski, "Performance of a hierarchical cellular network with mobility-dependent handover strategies," in *Proceedings of the Vehicular Technology Conference*, 1996, pp. 1868-1872.
- [Lee02] Y. Lee, I. Park, and Y. Choi, "Improving TCP Performance in Multipath Packet Forwarding Networks," *Journal of Communication and Networks (JCN)*, Vol. 4, No. 2, pp.148-157, June 2002.
- [Lee06] K.-W. Lee, J.-Y. Ko, Yong-Hwan Lee, "Fast Cell Site Selection with Interference Avoidance in Packet Based OFDM Cellular Systems", *Global Telecommunications Conference*, 2006.
- [Leung07] K.-C. Leung, V. O. K. Li, and D. Yang, "An Overview of Packet Reordering in Transmission Control Protocol (TCP): Problems, Solutions, and Challenges," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 18, Issue 4, pp. 522-535, April 2007.
- [LGS07] J. Ledlie, P. Gardner and M. Seltzer, Network coordinates in the wild, Proc. USENIX Conf. (2007) 299-311
- [Li08] B. J. Li and C. L. Soung, Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks. *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 7, no. 1, January 2008
- [Li09] Hua Li, Md. Humayun Kabir, Takuro Sato. "Velocity adaptive vertical handoff on multi-frequency system". In *Proceedings of PIMRC'2009*, pp.773-777.
- [Lima07] S. R. Lima, P. Carvalho and V. Freitas, "Admission Control in Multiservice IP Networks: Architectural Issues and Trends", *IEEE Communications Magazine*, vol.45, no.4, pp.114-121, April 2007
- [Lohier08] S. Lohier, Y. Ghamri Doudane, and G. Pujolle, "Cross-layer design to improve elastic traffic performance in WLANs", *ACM International Journal of Network Management*, Volume 18 Issue 3, July 2008.
- [Lopez09] D. López-Pérez et al., "OFDMA Femtocells: A Roadmap on Interference Avoidance," *IEEE Commun. Mag.*, vol. 47, no. 9, Sept. 2009, pp. 41–48.
- [LRL+10] K. Lee, I. Rhee, J. Lee, S. Chong, and Y. Yi, "Mobile data offloading: how much can WiFi deliver?" in *Proc. of Co-NEXT*. ACM, 2010, pp. 26:1–26:12.
- [Maheshwari09] R. Maheshwari, C. Jing and S.R. Das, "Physical Interference Modeling for Transmission Scheduling on Commodity WiFi Hardware", In Proc. of IEEE INFOCOM '09, 2009
- [Mahmoud10] H. Mahmoud, I. Güvenc, and F. Watanabe, "Performance of Open Access Femtocell Networks with Different Cell-Selection Methods," in Proc. of the *71st IEEE Vehicular Technology Conference (VTC)*, May 16–19 2010, pp. 1–5.
- [Mathar02] R. Mathar and M. Schmeink, "Integrated optimal cell site selection and frequency allocation for cellular radio networks," *Telecommunication Systems*, vol. 21, pp. 339–347, 2002.
- [MCK04] J. Mogul, Y. Chan and T. Kelly, Design, Implementation and evaluation of duplicate transfer detection in HTTP, Proceedings 1. Symposium on Network Systems Design and Implementation (2004) 43-56
- [McNair04] Janise McNair and Fang Zhu. Vertical handoffs in fourth-generation multinet network environments. *Wireless Communications, IEEE*, 11(3):8–15, June 2004.
- [Menth08] M. Menth, S. Kopf, J. Charzinski and K. Schrod, "Resilient network admission control", *Comput. Netw.*, vol.52, no.14, pp. 2805-2815, October 2008.
- [Menth10] M. Menth, F. Lehrieder, B. Briscoe, P. Eardley, T. Moncaster, J. Babiarz, A. Charny, X. Zhang, T. Taylor, K.-H. Chan, D. Satoh, R. Geib and G. Karagiannis, "A survey of PCN-based admission

control and flow termination“, IEEE Communications Surveys & Tutorials, vol.12, no.3, pp. 357-375, 2010.

[Moon10] J.-M. Moon and D.-H. Cho, “Efficient Cell Selection Algorithm in Hierarchical Cellular Networks: Multi-User Coordination,” IEEE Communication Letters, Vol. 14, No. 2, February 2010.

[Moon10a] J.-M. Moon and D.-H. Cho, “Cell Selection Algorithm Based on Competition of Users in Hierarchical Cellular Networks,” *IEEE WCNC*, 2010, pp. 1–6.

[Morimoto_09] A. Morimoto et al.: "Investigation on Optimum Radio Link Connection Using Remote Radio Equipment in Heterogeneous Network for LTE-Advanced", IEEE Vehicular Technology Conference, 26-29 April 2009, Barcelona, Spain, pp. 1-5

[Mortier00] R. Mortier, I. Pratt, C. Clark, and S. Crosby, "Implicit admission control“, IEEE Journal on Selected Areas in Communications, vol.18, no.12, pp.2629-2639, Dec 2000.

[MRT10] “ALTO in Mobile Core”, Y. El Mghazli, S. Randriamasy, F. Taburet, Alcatel-Lucent Bell Labs France, October 23 2010, <http://tools.ietf.org/html/draft-randriamasy-alto-mobile-core-01>

[Neu_Mobile_09] Neu Mobile Ltd, Mobile Traffic Growth + Cost Pressures = New Solutions? – Aug. 2009. [Online:] http://www.neu-mobile.com/report_finalv2.pdf (Accessed: July. 12, 2011)

[NokiaSiemensNetworks_1] Mobile broadband with HSPA and LTE –capacity and cost aspects (whitepaper) <<http://www.nokiasiemensnetworks.com/>>.

[NokiaSiemensNetworks_2] Nokia Siemens Networks, “Improving 4G coverage and capacity indoors and at hotspots with LTE femtocells”, White paper (2011) <<http://www.nokiasiemensnetworks.com/>>.

[PFA+10] I. Poesse, B. Frank, B. Ager, G. Smaragdakis, A. Feldmann, Improving content delivery using provider-aided distance information, Proc. Internet Measurement Conference IMC’10, Melbourne, Australia (2010) 22-34

[Qu10] T. Qu, D. Xiao ,D. Yang, “A novel cell selection method in heterogeneous LTE-advanced systems”, *Proceedings of IEEE IC-BNMT2010*, pp.510-513, 2010.

[Radunovic08] B. Radunovic, C. Gkantsidis, D. Gunawardena, and P. Key, "Horizon: Balancing TCP over Multiple Paths in Wireless Mesh Network," 14th Annual International Conference on Mobile Computing and Networking (MobiCom 2008), 14-19 September 2008.

[Randriamasy12] S. Randriamasy (editor) and N. Schwan, “ALTO Cost Schedule”, IETF draft draft-randriamasy-alto-cost-schedule-00, March 5 2012, Presented at the 83rd IETF, Paris (March 2012), <http://tools.ietf.org/id/draft-randriamasy-alto-cost-schedule-00.txt>

[Randriamasy12-2], S. Randriamasy (editor) and N. Schwan, “ALTO Cost Schedule 02”, IETF draft draft-randriamasy-alto-cost-schedule-02, October 19th 2012, scheduled at the 85th IETF, Atlanta GA, <http://tools.ietf.org/html/draft-randriamasy-alto-cost-schedule-02>

[RAN11] “Multi-Cost ALTO”, S. Randriamasy, Alcatel-Lucent Bell Labs France, July 11 2011, <http://tools.ietf.org/id/draft-randriamasy-alto-multi-cost-03.txt>

[REE01] W.J. Reed, The Pareto, Zipf and other power laws, Economics Letters 74 / 1 (2001) 15-19

[RFC3261] J. Rosenberg et al: “SIP: Session Initiation Protocol”, IETF RFC 3261, June 2002, <http://tools.ietf.org/html/rfc3261>.

[RFC3588] P. Calhoun et al.: “Diameter Base Protocol”, IETF RFC 3588, Sept. 2003, <http://tools.ietf.org/html/rfc3588>. [RFC4655] A. Farrel, J.-P. Vasseur, and J. Ash, A Path Computation Element (PCE)-Based Architecture, IETF RFC 4655, August 2006. <http://tools.ietf.org/html/rfc4655>.

[RFC4960] R. Stewart (Ed.), Stream Control Transmission Protocol, IETF RFC 4960, September 2007. <http://tools.ietf.org/html/rfc4960>.

[RFC5245] J. Rosenberg: “Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols”, IETF RFC 5245, Apr. 2010, <http://tools.ietf.org/html/rfc5245>.

[RFC5389] J. Rosenberg et al.: “Session Traversal Utilities for NAT (STUN)”, IETF RFC 5389, Oct. 2008, , <http://tools.ietf.org/html/rfc5389>.

[RFC5555] H. Soliman (editor), “Mobile IPv6 Support for Dual Stack Hosts and Routers”, IETF RFC 5555, June 2009, <http://tools.ietf.org/html/rfc5555>. [RFC6089] G. Tsirtsis, H. Soliman, N. Montavont, G. Giarretta, K. Kuladinithi, “Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support”, IETF RFC 6089, January 2011, <http://tools.ietf.org/html/rfc6089>. [RFC6372] N. Sprecher (Ed.) and A. Farrel (Ed.), “MPLS Transport Profile (MPLS-TP) Survivability Framework”, IETF RFC 6372, September 2011, <http://tools.ietf.org/html/rfc6372>. [Sakellari10] G. Sakellari and E. Gelenbe, "A distributed admission control mechanism for multi-criteria QoS“, In Proc. of IEEE GLOBECOM 2010, Workshop on Advances in Communications and Networks, pp. 1195-1999, December 2010.

- [SAN10] Sandvine Inc., Fall 2010 global Internet phenomena report <www.sandvine.com> (2010)
- [SAN12] Sandvine Incorporated ULC: Solutions Overview. (2012); <http://www.sandvine.com/solutions/default.asp>
- [Sang04] A. Sang, X. Wang, M. Madhian, and R. D. Gitlin, "A Load-aware handoff and cell-site selection scheme in multi-cell packet data systems," in *Proceedings of the IEEE 47th Global Telecommunications Conference (GLOBECOM)*, vol. 6, 2004, pp. 3931–3936.
- [Sangiamwong11] J. Sangiamwong, et al., "Investigation on Cell Selection Methods Associated with Inter-cell Interference Coordination in Heterogeneous Networks for LTE-Advanced Downlink", *European Wireless 2011*, April 27-29, 2011.
- [SCK+09] A.-J. Su, D.R. Choffnes, A. Kuzmanovic and F.E. Bustamante, Drafting behind Akamai, *IEEE/ACM Trans. on Networking* 17 (2009) 1752–1765
- [SEH10+] "Interconnected Content Distribution in LTE Networks" C. Schwartz, J. Eisl, A. Halimiz, A. Rafetseder, and K. Tutschku, *IEEE GlobeCom 2010 Workshop on Advances in Communications and Networks (ACN 2010)*, Miami USA Dec. 6th – 10th
- [Shetty10] S. Shetty, T. Ying and W. Collani, "TCP Venoplus — A cross-layer approach to improve TCP performance in wired-cum-wireless networks using signal strength", in *proc. of International Conference of Networking, Sensing and Control (ICNSC)*, 2010
- [SHH07] H.M. Sigurdsson, U.R. Halldorsson and G. Haßlinger: Potentials and challenges of peer-to-peer based content distribution, *Telematics and Informatics*, Elsevier, Vol. 24 (2007) 348-365
- [Simsek11] M. Simsek, et al. , "Performance of different cell selection modes in 3GPP-LTE macro-/femtocell scenarios" , *IEEE Wireless Advanced (WiAd) 2011*, pp.126-131, June 2011.
- [Stevens-Navarro06] Enrique Stevens-Navarro and Vincent W.S. Wong. Comparison between vertical handoff decision algorithms for heterogeneous wireless networks. In *Proc of 63rd Vehicular Technology Conference, VTC 2006-Spring.*, volume 2, pages 947–951. IEEE, 2006.
- [Susitaival09] R. Susitaival and S. Aalto, Adaptive load balancing with OSPF, in *Traffic and Performance Engineering for Heterogeneous Networks*, ed. D.D. Kouvatsos, pp. 85 - 107, 2009, River Publishers, Gistrup, Denmark.
- [SYB+09] X. Shen, H. Yu, J. Buford and M. Akon (Eds.), *Handbook of peer-to-peer networking*, Springer (2009)
- [Taleb_11] T. Taleb, K. Samdanis, S. Schmid, "DNS-Based Solution for Operator Control of Selected IP Traffic Offload", *IEEE International Conference on Communications (ICC)*, ISBN: 978-1-61284-232-5, pp.1-5, 2011.
- [TFR+11] R. Torres, A. Finamore, Jin Ryong, Kim; M. Mellia, M. M. Munafo; Sanjay Rao "Dissecting Video Server Selection Strategies in the YouTube CDN" 2011 31st International Conference on Distributed Computing Systems (June 2011), pg. 248-257
- [Tongwei10] Tongwei Qu, Dengkun Xiao, Dongkai Yang, "A novel cell selection method in heterogeneous LTE-advanced systems", *Broadband Network and Multimedia Technology (IC-BNMT)*, 3rd IEEE International Conference on, 2010
- [Tran_Minh_Trung_11] Tran Minh Trung, Youn-Hee Han, Hyon-Young Choi, Hong Yong Geun, "A Design of Network-based Flow Mobility based on Proxy Mobile IPv6", In *proc. of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 373–378, ISBN: 978-1-4577-0249-5, April 2011.
- [TSTAT] Tstat Homepage, <http://tstat.polito.it>.
- [Tuffery_11] A. Tuffery et al.: "A 27.5-dBm linear reconfigurable CMOS power amplifier for 3GPP LTE applications", *IEEE New Circuits and Systems Conference (NEWCAS)*, 26-29 June 2011, Bordeaux, France, pp. 221-224
- [Wang_07] Q. Wang, R. Atkinson, C. Cromar, J. Dunlop, "Hybrid User- and Network-Initiated Flow Handoff Support for Multihomed Mobile Hosts", In *proc. of IEEE 65th Vehicular Technology Conference, VTC2007-Spring*, pp.748–752, ISBN: 1-4244-0266-2, April 2007.
- [Wang99] H. J. Wang, R. H. Katz, and J. Giese. Policy-enabled handoffs across heterogeneous wireless networks. In *WMCSA '99: Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications*, page 51, Washington, DC, USA, 1999. IEEE Computer Society.
- [Wee11] L. T. Wee, M. Portmann, and H. Peizhao, "A Systematic Evaluation of Interference Characteristics in 802.11-Based Wireless Networks" In *Proc. IEEE International Conference on Advanced Information Networking and Applications (AINA)*, 2011

- [WF10] F. Weiden, P. Frost, “Anycast as a load balancing feature” LISA'10 Proceedings of the 24th international conference on Large installation system administration
- [wikithc] <http://wiki.thc.org/vodafone>
- [Wind08] Windisch, G.: Vergleich von QoS- und Mobilitätsmechanismen in Backhaul-Netzen für 4G Mobilfunk; 2008
- [Wu08] D. Wu, P. Djukic, and P. Mohapatra, “Determining 802.11 link quality with passive measurements”, in *Proc. Wireless Communication Systems (ISWCS '08)*, 2008.
- [WW09] S. Wiethölter and A. Wolisz, “Selecting vertical handover candidates in IEEE 802.11 mesh networks,” in *Proc. of WoWMoM Workshops*. IEEE, June 2009, pp. 1 – 7.
- [Yilmaz05] O. Yilmaz, A. Furuskar, J. Pettersson, and A. Simonsson. Access selection in WCDMA and WLAN multi-access networks. In *Proc. of Vehicular Technology Conference, VTC Spring, IEEE*, volume 4, pages 2220–2224, 2005.
- [Yi-Neng_Lin_10] Yi-Neng Lin, Wen Chen, Shan-Chi Tsai, Yi-Bing Lin: Design and Implementation of An Offloading Technology for 3.5G Networks, IEEE 71st Vehicular Technology Conference (VTC 2010-Spring), pp. 1 – 5, May 2010.
- [Yokota_11] H. Yokota, D. Kim, B. Sarikaya, F. Xia, “Home Agent Initiated Flow Binding for Mobile IPv6”, IETF Internet Draft, December 22, 2011.
- [YSN10] X. Yan, Y. A. Sekercioglu, and S. Narayanan, “A survey of vertical handover decision algorithms in Fourth Generation heterogeneous wireless networks,” *Computer Networks*, vol. 54, no. 11, pp. 1848 – 1863, 2010.
- [Zhao11] L. Zhao, X. Li, T. Weerawardane, A. Timm-Giel and C. Görg, Joint Load Balancing of Radio and Transport Networks in LTE System, in Third International Conference on Ubiquitous and Future Networks (ICUFN 2011), Dalian, China, June 15-17, 2011.
- [ZKG10] R. Zhou, S. Khemmarat, and L. Gao, “The Impact of YouTube Recommendation System on Video Views,” IMC '10: Proceedings of the 10th annual conference on Internet measurement, 2010.
- [ZSG+08] M. Zink, K. Suh, Y. Gu, and J. Kurose, “Watch Global, Cache Local: YouTube Network Traffic at a Campus Network-Measurements and Implications,” Proceedings of the 15th SPIE/ACM Annual Multimedia Computing and Networking Conference (MMCN), 2008.
- [Xia10] R. Xia and J. Muppala, “A survey of bittorrent performance,” *Communications Surveys Tutorials*, IEEE, vol. 12, pp. 140-158, quarter 2010.
- [Perez09] G. R. D. Lopez-Perez, A. Valcarce and J. Zhang, “Ofdma femtocells: A roadmap on interference avoidance,” *IEEE*, vol. 47, no. 9, pp. 41–48, 2009.
- [Okino11] K. Okino, T. Nakayama, C. Yamazaki, H. Sato, and Y. Kusano, “Pico cell range expansion with interference mitigation toward lte-advanced heterogeneous networks,” 2011.
- [Rong12] Q. Ye, B. Rong, Y. Chen, M. Al-Shalash, C. Caramanis, and J. G. Andrews, “User association for load balancing in heterogeneous cellular networks,” *CoRR*, vol. abs/1205.2833, 2012.
- [Eck12] M. Eckert, T.M. Knoll, “ISAAR (Internet Service quality Assessment and Automatic Reaction)”, Monami 2012

1 Appendix: IETF standardization on traffic management

1.1 IETF ALTO protocol in a 3GPP study item on IMS based P2P

The 3GPP has started a study in October 2011 that is reported in [3GPP_TR_23.844] and introduced as follows:

“This study focuses on the enhancement of IMS to support Peer-to-Peer Content Distribution Services in respect of GPRS, EPC and other underlying access network technologies but not intend to modify GPRS or EPC for P2P mechanism. The objectives are to study IMS based Peer-to-Peer Content Distribution Services on the architectural level with the following aspects:

- Creating solutions in order to fulfill the use cases and requirements as defined by SA1 while avoiding duplicate work in other SDOs, such as IETF [e.g., PPSP, P2PSIP, ALTO, and DECADE], and re-using their work. The solutions should:
 - Apply the same IMS user management/registration procedure as other IMS services;
 - Be able to provide the UE with the appropriate AS to obtain the addresses of other Peers, from which the UE can retrieve the requested content;
 - Re-use ISC interface for service triggering;
 - Be able to select qualified User Peers among available UEs according to the policies preconfigured in the network;
- Elaborate alternative solutions, which support the following network access technologies:
 - Mobile access only (e.g. UTRAN, E-UTRAN, I-WLAN);
 - Fixed access only (e.g. xDSL, LAN);
 - Fixed and mobile convergence scenarios.
- Evaluate possible impacts and improvements on network when IMS based Peer-to-Peer Content Distribution Services are deployed, such as the interactions that are needed to adapt the peer-to-peer overlay properties to the configuration and the resources of the network.
- Identify QoS, mobility, charging and security related requirements in the case of Peer-to-Peer Content Distribution Services on IMS.

The assessment on alternative solutions and the final conclusion of this study should not only take TR 22.906 into consideration but also comply with the related normative work in SA1.”

1.1.1 Integration of ALTO in the IMS P2P Content Distribution Service

The Integration of ALTO in the IMS P2P Content Distribution Service is described in [3GPP_TR_23.844]. The study considers content delivery services (CDS) for large data volumes like content on demand, video streaming. The IMS P2P CDS system is required in particular to:

- Support a mechanism to provide address information for accessing an IMS based P2P content distribution service for an IMS P2P CDS UE.
- Support a mechanism to provide to User Peers an optimal selection of User Peers and Network Peers for obtaining requested media content from, based upon metrics including access type, offloading capability and traffic conditions.
- Provide QoS

To support this, three alternatives, including architecture and information flows are proposed and described in Sections 6.1, 6.2 and 6.3 of [3GPP_TR_23.844].

TITRE 4 Including an ALTO Server in IMS P2P CDS

The use of the ALTO protocol and inclusion of an ALTO Server in the architecture is described in Section 6.5 of [3GPP_TR_23.844] and summarized below.

User peers and network peers may query an ALTO (Application Layer Traffic Optimization) Server for cost values between peers in a swarm to be used to rank a list of peers of the requested content as described in draft-ietf-alto-protocol [ALI11]. A query may consist of a peer's location and the type of information the peer requires from the ALTO Server. An ALTO Server may provide the following:

- a Cost Map which may rank available peers for the requested content in a specific order depending on the cost metric used, e.g. routing hop count, access network characteristics, peer battery capabilities,
- a Network Map which may consist of a list of peer identities and/or peer IP addresses, or peers in close proximity to the peer requesting content, e.g. same cell, same access, or same operator domain.

An ALTO server may obtain information from a Tracker AS, HSS, and other sources such as distributed hash tables which may or may not be a part of the IMS architecture.

ALTO client to ALTO server communication may traverse IMS entities.

In the case of a list of peers from which content is available to an IMS P2P CDS UE, information from the ALTO server can aid the IMS P2P CDS UE to determine the optimal set of peers to contact in order to retrieve the desired content segments. Figure 1-1 below shows the interaction between ALTO client and ALTO server, and describes the content of the messages exchanged between these entities.

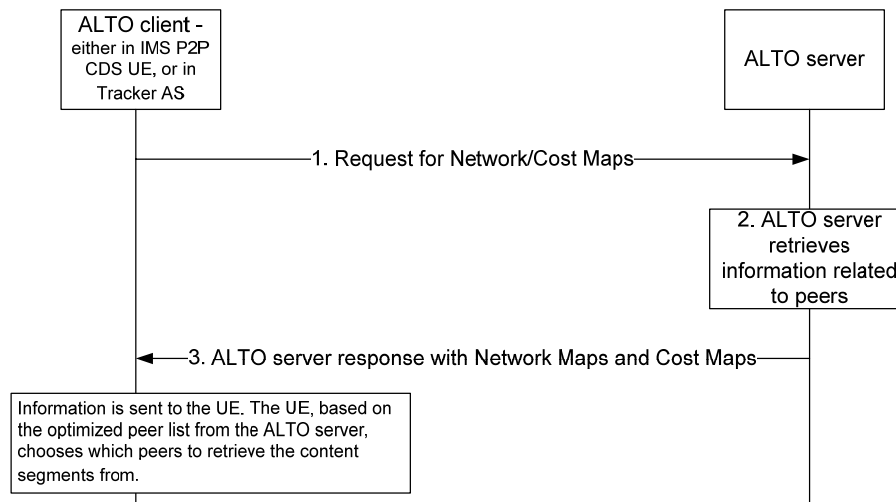


Figure 1-2 ALTO message exchange for peer list optimization

The ALTO client, residing in either the IMS P2P CDS UE, or in the Tracker AS, sends a request for Network/Cost maps to the ALTO server. The following information may be included in the request:

- the request includes the peer list retrieved from the Tracker AS,
- indications of what information is desired from the ALTO server. The following can be requested from the ALTO server:
 - Network Map – grouping peers from the peer list – grouping can be for example per cell ID, per access type, per network domain;
 - Cost Map, including path costs for the peers such as hop count from the IMS P2P CDS UE, or physical proximity (e.g. determined by geolocation);
- the client may ask for properties of the peers in the peer list such as the access over which peers are connected.

2. The ALTO server retrieves information related to peers.

3. The ALTO server organizes the peers in the peer list into groups and assigns a cost weighting to each group and/or each peer according to the cost type requested. Also provided is the cost mode to indicate if the cost weighting is a numerical value or an ordinal/ranking value.

The ALTO client may query the ALTO server subsequently, in order to retrieve updated metrics on peers, since the Cost Map may have changed due to the dynamic nature of peers and the IMS P2P CDS UE.

1.1.2 Status

The mechanisms by which the ALTO server retrieves peer related information is for further study.

The last updates have been observed in February 2012 and are documented in 3GPP architecture. They are documented in the 3GPP temporary documents (TD). They relate to: the ALTO Service architecture see TD [S2-120623], the ALTO Redirection procedure see TD [S2-120624] and other ALTO sections of [3GPP_TR_23.844] see TD [S2-120671].

Note that ALTO metrics such as peer battery capabilities foreseen for this IMS use case are not yet considered or specified in the ALTO WG. However this study item provides a valuable use case to motivate possible related protocol extensions.

1.2 Relevance for Mevico WP4

Where as one key objective of Mevico is to enhance the EPC architecture to support contemporary applications such as IMS based P2P, the objective of this 3GPP study is to enhance IMS based P2P so as to support mobile, fixed and converged access technologies. At the end of this study, the assumption is that the enhanced application architecture is considered a reference against which the evolutions proposed in the Mevico project can be tested and evaluated.

As for ALTO, this study clearly shows:

- The relevance of ALTO to efficiently optimize applications and its specification generic enough to allow its applicability to various network access technologies and gain traction in the 3GPP where total consensus is the rule.
- The relevance of using the ALTO protocol to support IMS based P2P, that itself is suited to EPC access technologies.

2 Appendix: 3GPP standardization on traffic management

2.1 SAE Network Architecture

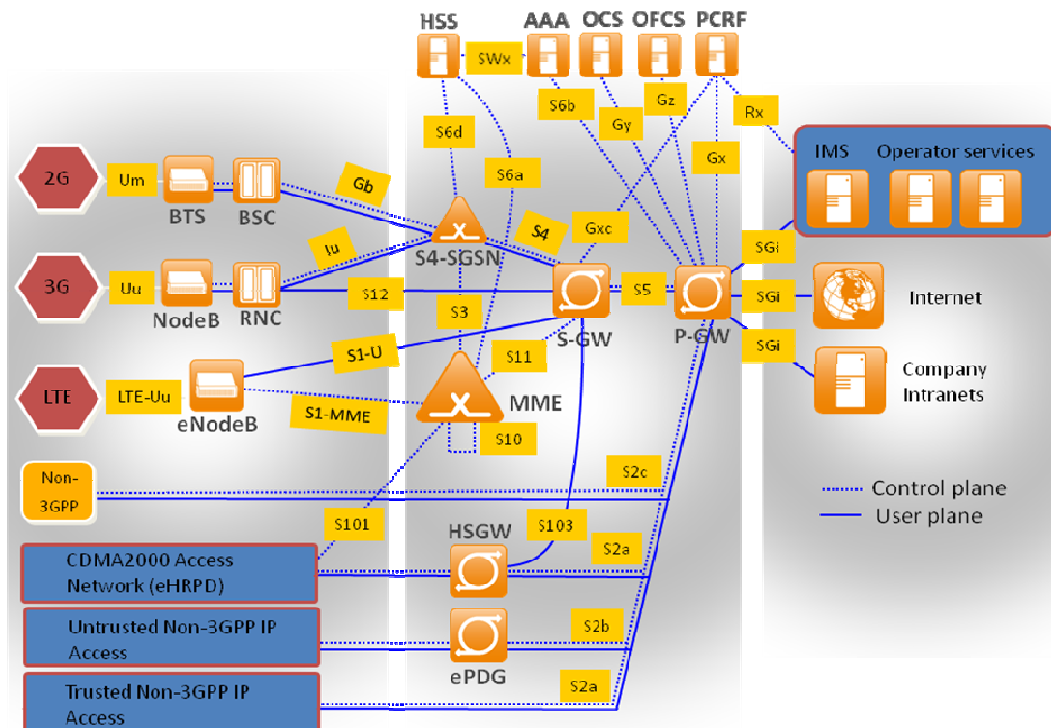
2.1.1 Introduction

Main drivers for evolution of mobile networks are higher bandwidth and improving the spectral efficiency (data rate per bandwidth). After improving these key factors for WCDMA over several years by introducing HSPA and HSPA+, end of 2004 the 3rd Generation Partnership Project (3GPP) standardization forum started evaluating a new radio technology as successor for WCDMA providing even higher peak data rates (>100 Mbit/s Downlink, >50 Mbit/s Uplink) and lower latency besides other improvements. This work was called Long Term Evolution (LTE) and is nowadays the radio interface name used in most official publications. Inside 3GPP the radio access network is called Evolved UMTS Radio Access Network (E-UTRAN) to indicate the path from GERAN (GSM/GPRS/EDGE) to UTRAN (WCDMA/HSPA) and finally to E-UTRAN (LTE). In parallel to the work on a new radio interface, 3GPP initiated a study to evolve the 2G/3G packet core network (known as GPRS core) in order to cope with the new demands of LTE. This core network study was called System Architecture Evolution (SAE) and it was documented in the Technical Report [3GPP_TR_23.882]. The outcome of this work is a new packet core design in Release 8 documented in Technical Specifications [3GPP_TS_23.401] and [3GPP_TS_23.402] and is called the Evolved Packet Core (EPC). 3GPP Release 8 was officially completed in March 2009. EPC allows connecting LTE, GERAN/UTRAN, non-3GPP access systems like WLAN, WiMAX and CDMA as well as 3GPP compliant small Femto Access Points installed at home or inside companies. Special emphasis was put on optimized handover procedures between LTE and CDMA2000 eHRPD (Evolved High Rate Packet Data) accesses due to requirements from some CDMA network operators in the US and Japan, who intended to start with LTE in 2010. The EPC together with these access systems is called Evolved Packet System (EPS). In contrast to the 2G and 3G systems, EPS does no longer contain a circuit switched part.

LTE/SAE has evolved from the 2G/3G PS domain, and EPC has its roots in the GPRS (General Packet Radio System) core network. Separation of control and user plane functions was a key in the design of EPC, thus the EPC consists basically of three functional elements. One is the Mobility Management Entity (MME) that resides in the control plane of EPC. The MME can be seen as an evolution of the SGSN (Serving Gateway Support Node) control plane function in GPRS. The Serving Gateway (S-GW) correlates with the SGSN user plane function in GPRS. All user plane packets in UL and DL are traversing the S-GW and the S-GW also acts as a local mobility anchor that is able to buffer downlink packets during handover. The PDN Gateway (P-GW) finally is the global IP mobility anchor point comparable to the GGSN (GPRS Gateway Support Node) in GPRS. It allocates IP addresses to UEs and provides the interface towards PDNs like the Internet or the mobile operator's service domain. The P-GW also contains the Policy Enforcement Function (PECF) for the detection of service data flows, policy enforcement (e.g. discarding of packets) and flow based charging. All these network elements are logical functions, i.e. in real implementations two or more functions (e.g. S-GW and P-GW) can reside on the same physical hardware platform. While the MME is selected by the eNodeB for a new session, the MME itself selects S-GW and P-GW by constructing special domain names and resolving these names by means of the operator's DNS infrastructure. In the following we will describe the EPS architecture variants for non-roaming and roaming cases and the architectures for interworking to 2G/3G and non-3GPP access systems.

2.1.2 Non-Roaming Architecture

The following figure gives an overview of the logical LTE/SAE architecture in the non-roaming case, i.e. the UE is served by its HPLMN. To provide a full picture also non-3GPP access systems and corresponding interfaces are shown. Among the non-3GPP access systems, special emphasis was put on CDMA2000 access networks with new interfaces S101 and S103 to speed up handover between CDMA2000 eHRPD access and LTE. For completeness this figure shows also some of the charging relevant interfaces.



Besides MME, S-GW and P-GW, a couple of other logical functions are part of the EPC. The Home Subscriber Server (HSS) contains all subscription relevant data of the users like IMSI, MSISDN, subscribed APN, priority indication and more. As the MME, similar to SGSN and MSC, is responsible to authenticate the user and authorize the user's request to access network resources (e.g. authorizing the APN provided by the UE), the MME needs access to these subscription data stored in the HSS. The HSS stores the addresses of the MME serving a particular UE.

The Policy and Charging Rules Function (PCRF), as further detailed in the PCC clause below, translates session data coming from the application layer (e.g. content of SDP in SIP signalling) into access specific parameters and provides these parameters together with charging relevant data in so-called PCC rules to the Policy Enforcement Function (PCEF), which is part of the P-GW. If GTP is used between S-GW and P-GW (by far the predominant use case) QoS rules like the maximum bit rate in DL and UL are also provided from PCRF to P-GW/PCEF as GTP (GPRS Tunnel Protocol) allows for establishing bearers with respective QoS. If an operator decides to use PMIP (Proxy Mobile IP) between S-GW and P-GW, the bearers are terminated in the S-GW instead of the P-GW, because a bearer concept is not known to PMIP. Thus, QoS rules have to be provided from PCRF to S-GW while policy and charging rules, which are applicable to single service flows, are still provided to the P-GW.

The AAA (Authentication Authorization and Accounting) server is either used to authenticate and authorize users who are accessing the EPC through non-3GPP access systems or, optionally, by the P-GW to authorize the provided APN (Access Point Node) and to allocate an IP address to the UE. The Evolved Packet Data Gateway (ePDG) terminates a secure tunnel from the UE in the EPC if the UE is camping on an un-trusted non-3GPP access system. Within the secure tunnel the control and the user plane messages are exchanged.

The SGSN as shown in the above figure (also called S4-SGSN) is enhanced to have a direct interface with the S-GW to manage bearers and possibly forward user plane traffic (depending on whether a Direct Tunnel is used between RNC and S-GW or not). Thus the S4-SGSN behaves similar like the MME towards the EPC but provides Iu interface to UTRAN and Gb interface to GERAN.

The Online Charging System (OCS) performs real-time credit control. Its functionality includes e.g. transaction handling, rating, online correlation and management of subscriber accounts and balances. The Offline Charging System (OFCS) collects charging relevant data from network elements and passes them to the operator's billing domain to generate subscriber billing records.

The eHRPD Serving Gateway (HSGW) as part of the CDMA2000 eHRPD network ensures converged mobility management between eHRPD and LTE networks. The HSGW provides for interworking between eHRPD access nodes and P-GW.

When data forwarding is used as part of mobility procedures different user plane routes may be used based on the network configuration (e.g. direct or indirect data forwarding).

2.1.3 Roaming Architecture (home routed)

The roaming architecture, i.e. the UE is served by a VPLMN, is similar to the non-roaming architecture. The main difference is that in the roaming case the S-GW is located in the VPLMN while the P-GW is (usually) located in the HPLMN as most of the traffic is home routed traffic. If local breakout is used, the P-GW is located in the VPLMN, but this scenario requires special arrangements between operators (e.g. usage of special APNs, providing charging tickets from P-GW in VPLMN to HPLMN) and the user must be subscribed to this service. Thus, home routed traffic is the dominant usage scenario for PS services by today and also in the near future. The roaming architecture in the home routed scenario is shown in the following figure.

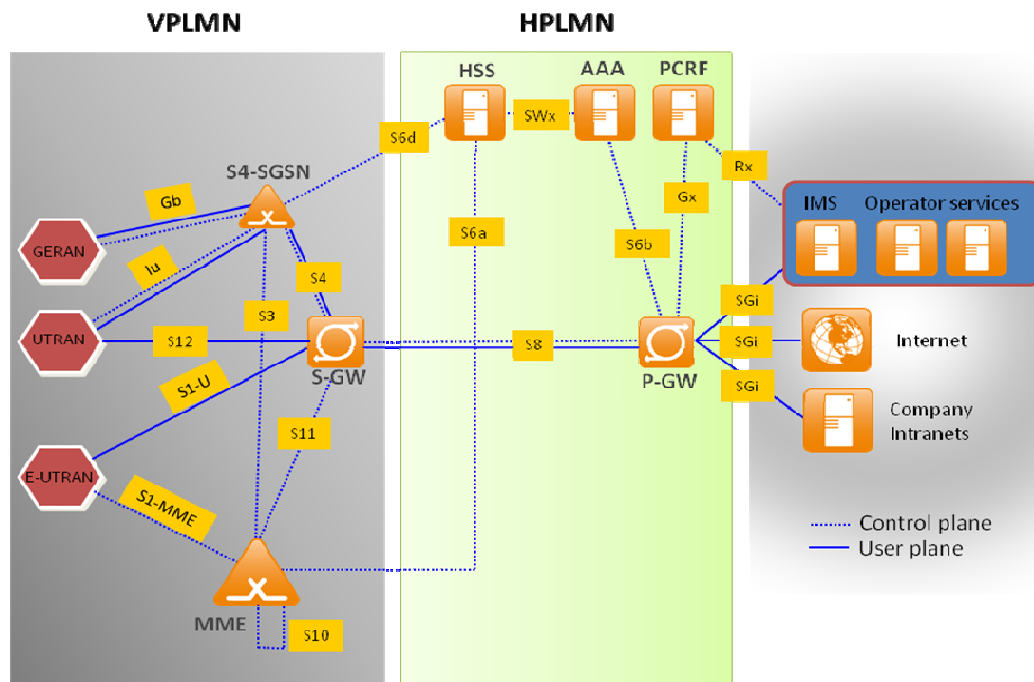


Figure A3-2: LTE/SAE roaming architecture - home routed case

As can be seen from the figure, the S5 interface is replaced by S8 in the roaming case and in fact both are providing nearly identical functionality. This is similar to usage of Gn/Gp interfaces in 2G/3G. S8 is either based on GTP or PMIP like S5; as PMIP is not widely used by operators GTP is more common.

2.1.4 Roaming Architecture (local breakout)

Finally the figure below shows the roaming architecture for local breakout. The key point in this scenario is that both the P-GW and the PCRF (V-PCRF) are located in the VPLMN connected via the Gx interface (Gx is not an inter-operator interface). In order to receive QoS rules from the HPLMN where the subscription data is stored (e.g. the subscribed maximum bit rate), a new interface S9 was introduced that connects the Home PCRF (H-PCRF) in HPLMN with the V-PCRF in VPLMN. A standardized solution to select a P-GW in the VPLMN does still not exist due to lack of operator interests (charging is one issue, loosing revenue and control to the roaming operator is another one). One possible solution would be to use specially constructed APNs, requested by the UE and used in the VPLMN to resolve them to a P-GW address in the roaming network. As shown in the figure below, the user can potentially use operator services in the HPLMN or in VPLMN when local breakout is deployed.

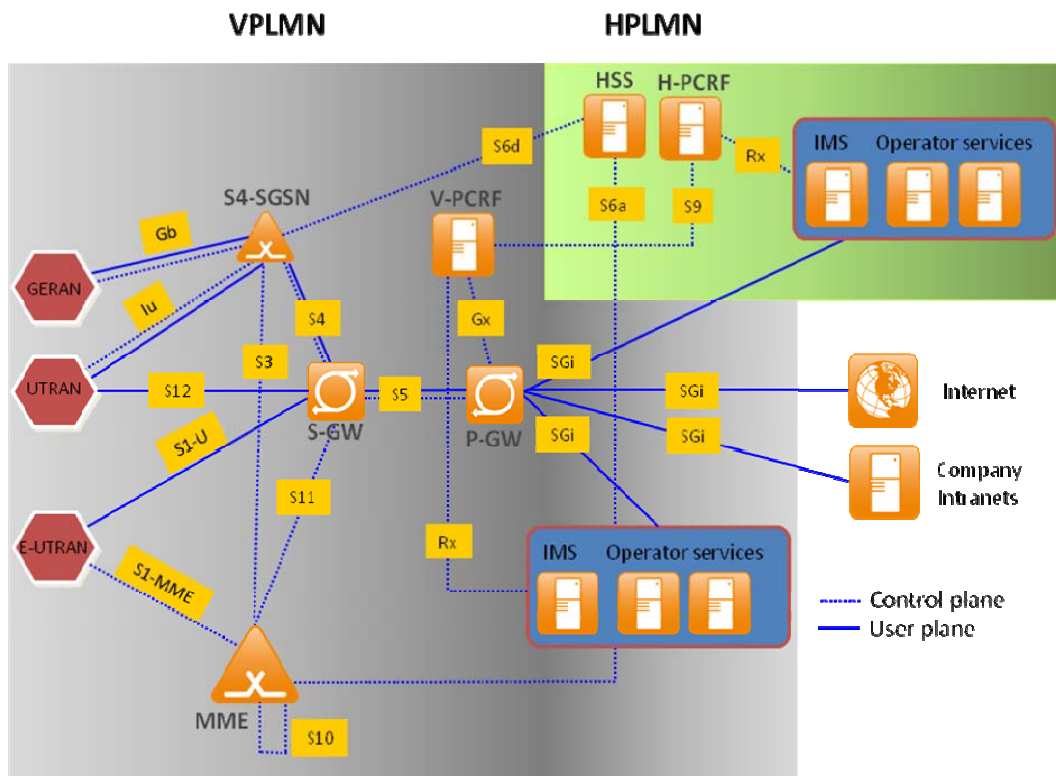


Figure A3-3: LTE/SAE roaming architecture – local breakout case

2.1.5 Relevance for MEVICO WP4

Understanding the SAE architecture is essential when discussing possible enhancements in the scope of WP4.

The 3GPP EPC already allows connecting LTE, GERAN/UTRAN, non-3GPP access systems like WLAN, WiMAX and CDMA and also 3GPP compliant small Femto Access Points installed at home or in companies. The P-GW is used as interconnection point towards IP networks, and all user plane traffic is routed through it. The P-GW handles the traffic according the operator-controlled policies that it may obtain them from the PCRF.

2.2 QoS and EPS Bearers

2.2.1 Session and Bearer Management

Session and Bearer Management Procedures are performed upon establishing a valid context between the UE and the MME. The default EPS bearer context is activated during the EPS Attach procedure. Upon successful attach, the UE can request the MME to set up connections to additional PDNs (Packet Data Networks, e.g. the public internet, IMS (IP Multimedia Sub-System) or an enterprise network). For each additional PDN connection, the MME activates a separate default EPS bearer. A default EPS bearer context remains activated throughout the lifetime of the connection to the PDN.

A dedicated EPS bearer context is always linked to a default EPS bearer context and represents additional EPS bearer resources between the UE and the PDN. The network can activate dedicated EPS bearer contexts together with the activation of the default EPS bearer context or at any time later, as long as the default EPS bearer context remains activated. Dedicated bearers are used when applications (e.g. IMS voice) have special QoS requirements.

Default and dedicated EPS bearer contexts can be modified. Dedicated EPS bearer contexts can be released without affecting the default EPS bearer context. If the default EPS bearer context is released, then all dedicated EPS bearer contexts linked to it are also released.

2.2.2 QoS Concept

The EPS provides IP connectivity between a UE and an external packet data network like the public internet. This is referred to as the PDN connectivity service. For EPC, this is provided by either an EPS bearer for GTP-based S5/S8 or by an EPS bearer concatenated with IP connectivity between S-GW and P-GW for PMIP-based S5/S8. An EPS bearer uniquely identifies traffic flows (i.e. one or more user

services) that receive a common QoS treatment. The EPS bearer traffic flow template (TFT) is the set of all packet filters associated with that EPS bearer.

The EPS bearer is the level of granularity for QoS control on bearer level in the EPC/E-UTRAN. All traffic mapped to the same EPS bearer receives the same bearer level packet forwarding treatment. Providing different bearer level packet forwarding treatment requires separate EPS bearers.

One EPS bearer is established when the UE connects to a PDN and that remains established throughout the lifetime of the PDN connection in order to provide the UE with always-on IP connectivity to that PDN. This bearer is referred to as the default bearer. Any additional EPS bearer that is established for the same PDN connection is referred to as a dedicated bearer. Service Data Flows (SDFs) with different QoS requirements can use different EPS bearers.

The role of and the requirements to the UE in the QoS handling are minimized in EPS. In general, the UE does not have to know about the QoS on the bearer level. Bearer resources in EPS are controlled by the network, i.e. the decision to establish or modify a dedicated bearer can only be made by the EPC. The EPC network establishes dedicated bearers (for SDF requiring a different QoS than offered by the existing bearer(s)) based on resource requests from the UE. Bearer level QoS parameter values are always assigned by the EPC [3GPP_TS_23.401].

However, the UE can also request the network to allocate, modify or release additional EPS bearer resources. The network decides on whether a request fulfills the condition for additional resources by activating a new dedicated EPS bearer context or by modifying an existing dedicated or default EPS bearer context.

The UE routes uplink packets to the different EPS bearers based on uplink packet filters in the TFTs assigned to the EPS bearers. The P-GW routes downlink packets to the different EPS bearers based on the downlink packet filters in the TFTs assigned to the EPS bearers in the PDN connection. The distinction between default and dedicated bearers is transparent to eNodeB.

2.2.3 Characteristics of an EPS bearer

An EPS bearer is referred to as a GBR bearer if dedicated network resources with Guaranteed Bit Rate (GBR) are permanently allocated at bearer establishment / modification. Otherwise, an EPS bearer is referred to as a Non-GBR bearer. The default EPS bearer is always a Non-GBR bearer. A dedicated bearer can either be a GBR or a Non-GBR bearer.

The EPS bearer QoS profile includes the following:

QCI: Scalar that is used as a reference to access node-specific parameters that control the bearer level packet forwarding treatment. See further details below.

ARP: Contains information about the priority level (scalar), the pre-emption capability (flag) and the pre-emption vulnerability (flag). The primary purpose of the ARP is to decide whether a bearer establishment / modification request can be accepted or needs to be rejected due to resource limitations.

GBR: Denotes the bit rate that can be expected to be provided by a GBR bearer.

MBR: Limits the bit rate that be expected to be provided by a GBR bearer.

Following QoS parameters are applied to aggregated set of EPS bearers:

APN-AMBR: Limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the APN.

UE-AMBR: Limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers of a UE.

Compared to UMTS, the LTE QoS concept was simplified by replacing a number of QoS parameters used in the 2G/3G networks with a single QoS parameter, the QCI, in the non-access stratum of the EPS, as described in figure A3-4. The aggregate maximum bit rate was introduced for non-guaranteed bit rate bearers as a per APN parameter and as a per UE parameter [3GPP_TS_23.401], [3GPP_TS_24.301], [3GPP_TS_29.274].

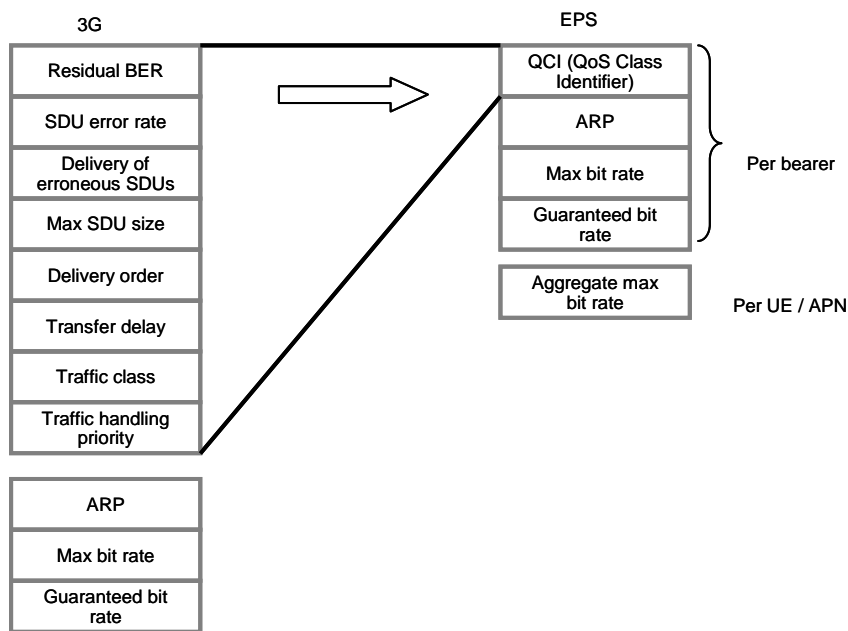


Figure A3-4: EPS QoS parameters vs. 3G QoS parameters

The QCI is scalar that is used as a reference to node specific parameters that control packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.) and that have been pre-configured by the operator owning the node (e.g. eNodeB). Standardized characteristics are associated with the standardized QCI values. These characteristics are guidelines for the pre-configuration of node specific parameters for each QCI. The reason for standardizing a QCI with corresponding characteristics is to ensure that applications and services mapped to that QCI receive the same minimum level of QoS in multi-vendor network deployments and in case of roaming. A one-to-one mapping of standardized QCI values to standardized characteristics is captured in Table 2-1 [3GPP_TS_23.203].

Table 2-1: Standardized QCI characteristics

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Application
1	GBR	2	100 ms	10^{-2}	Conversational Voice
2		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3		3	50 ms	10^{-3}	Real Time Gaming
4		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
5	Non-GBR	1	100 ms	10^{-6}	IMS Signalling
6		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file)
9		9			sharing, progressive video, etc.

2.2.4 Relevance for MEVICO WP4

Understanding the 3GPP SAE QoS concepts is essential for discussing possible enhancements in the scope of WP4.

QoS differentiation is provided within the 3GPP EPC by the distribution of traffic data flows to different bearers. The P-GW selects the bearers for downlink traffic data flows and also provides instructions to the UE how to put uplink traffic data flows to different bearers. The P-GW applies operator defined policies when selecting the QoS parameters for traffic data flows by using information received from the PCC framework. The UE may provide suggestions to about the QoS requirements to the P-GW and the PCC framework but the network has the final decision. Resource allocation and traffic scheduling in the radio network takes the QoS parameters of a bearer and the radio load situation into account.

2.3 Policy and Charging Control (PCC)

2.3.1 Architecture

3GPP recognized the importance and benefits of standardized service based Policy and Charging Control (PCC). Fair and flexible charging and proper Quality of Service (QoS) based on optimal and flexible usage of network resources are essential for both the end users and mobile operators.

From 3GPP Rel-7 onwards, the basic PCC architecture depicted in figure A3-5[3GPP_TS_23.203] applies.

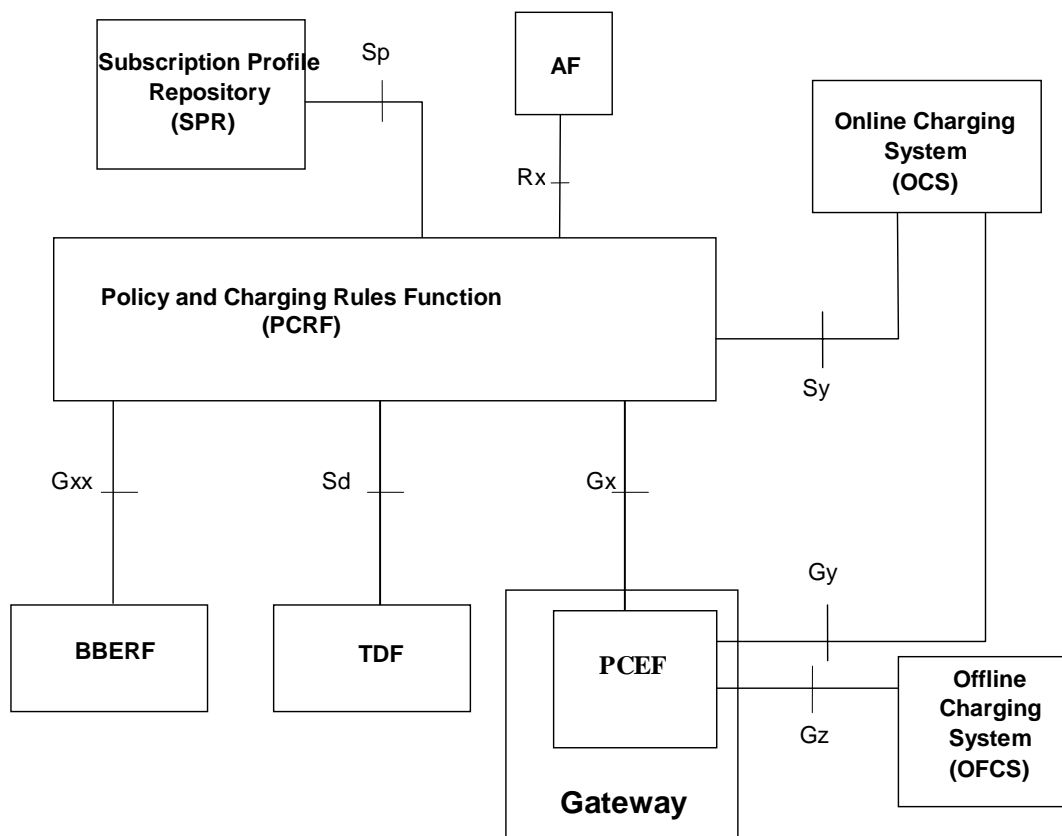


Figure A3-5: Policy and charging control architecture [3GPP_TS_23.203]

The architecture contains the following entities:

The **Policy and Charging Rules Function (PCRF)** generates policy (e.g. applicable QoS) and charging related information and provides them towards the PCEF. Rel-8 added support for local breakout scenarios where the PCEF resides in the visited network: The **V-PCRF** in the visited network controls the PCEF (and possibly the BBERF) and interacts with the **H-PCRF** in the home network via the S9 interface [3GPP_TS_29.215] (not depicted in the figures above).

The **Policy and Charging Enforcement Function (PCEF)**, processes user plane data according to given policies and collects related charging information. The PCEF is integrated into the GGSN or P-GW from Rel-8 onwards and can adjust the QoS of an IP-CAN bearer (e.g. EPC bearer context) used to transport

user plane data. The PCRF interacts with the PCEF via the Diameter based Gx interface [3GPP_TS_29.212].

In Rel-8, a new functional element, the **Bearer Binding and Event Reporting Function (BBERF)**, was specified for scenarios where an IP tunnel (instead of the GTP protocol) is used on the S5 interface between the packet data network gateway and the access network. The BBERF is located in the serving gateway SGW (for non-GTP 3GPP access) or in the access network gateway AGW (for non-3GPP accesses). The main functions of the BBERF are to bind Service data Flows (SDFs) to bearers with appropriate QoS and to report bearer level events to the PCRF. These functions cannot be carried out by the PCEF due to the IP tunnel. The BBERF is connected to the PCRF via a Diameter based Gxx interface which is a QoS related subset of the QoS and charging control related Gx interface between the PCRF and the PCEF [3GPP_TS_29.212].

The Sp reference point allows the PCRF to request subscription information related to the IP-CAN transport level policies from the **Subscription Profile Repository (SPR)** as an input to select appropriate policies. (however, no protocol is standardized for the Sp reference point)

An **Application Function (AF)** can provide information about active applications with user plane traffic towards the PCRF via the Rx interface [3GPP_TS_29.214]; the P-CSCF (of IMS) is one example of an AF which derives application related information from SIP and SDP call control signaling. The PCRF uses the application related information to define appropriate policy information to be sent to the PCEF. For instance, when a VoIP call is initiated in the IMS, the P-CSCF notifies the PCRF, and the PCRF sends policy information about the required guaranteed bit rate and QoS information (e.g. from Rel-8 onwards QCI) towards the PCEF, which establishes a suitable dedicated IP CAN bearer (EPS bearer context).

The **Traffic Detection Function (TDF)**, which was added in Rel-11, performs extended packet inspection and can inform the PCRF when traffic related to a specific application is detected. The PCRF can then again adjust the policy information and provides it to the PCEF.

2.3.2 Basic features and operations

When a UE attaches to the network to establish a PDN connection, the BBERF and/or PCEF functionality in the relevant gateway acts as a Diameter client and establishes a Diameter session towards the PCRF over the Gxx/Gx interface to get authorization and QoS parameters for the default bearer establishment towards the PDN. The request to the PCRF contains at least the user identification, UEs IPv4 address and/or IPv6 prefix, IP-CAN type and radio access type, but may contain further information like the UE time zone, UE location information, PDN information and the bearer control mode supported by the UE and the access network, if available.

In its response the PCRF may provision PCC rules and authorized QoS for the default EPS bearer, including a non-guaranteed bit rate, QoS class (QCI) and allocation and retention priority (ARP). The PCRF derives the selected bearer control mode based on the UE and access network information, subscriber information (which may be retrieved from the SPR) and operator policy. The bearer control mode options are: The UE requests resource establishment, modification or termination, or both the UE and the network may request resource establishment, modification or termination. The PCRF may provide event triggers to have the PCEF/BBERF re-request PCC/QoS rules when a certain event takes place on the user plane. The PCRF may provide charging related information to the PCEF, like the OFCS and/or OCS addresses defining the Offline and Online Charging system addresses, respectively, and the default charging method to indicate which charging method shall be used for each PCC rule [3GPP_TS_23.203], [3GPP_TS_29.212].

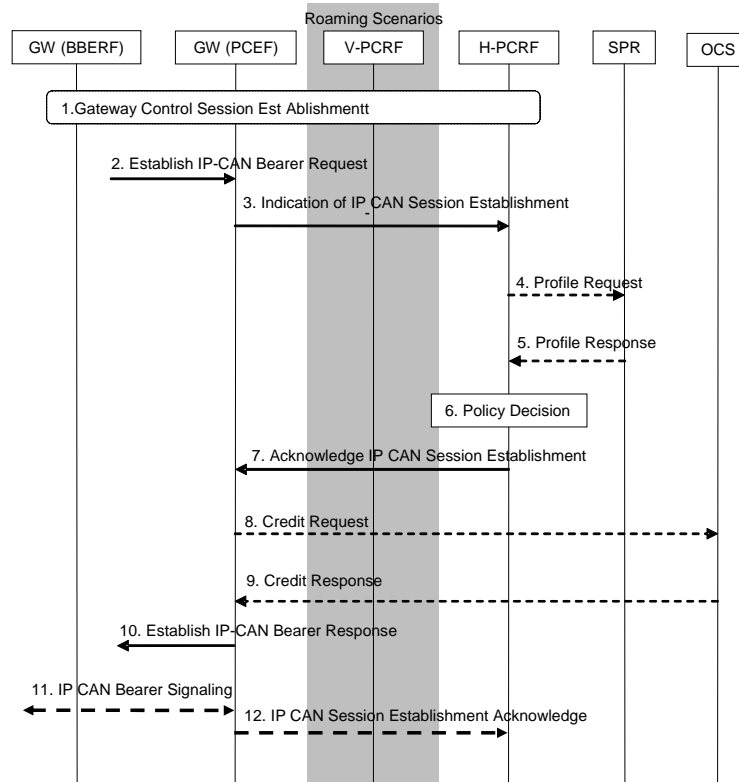


Figure A3-6: PCC related signalling upon an IP-CAN session establishment.

If Online Charging is applied and at least one PCC rule is activated by the response from the PCRF to the PCEF, the PCEF activates the online charging session towards the OCS and provides relevant input information for the OCS decision. Depending on operator configuration the PCEF may request credit from OCS for each charging key of the activated PCC rules. Figure A3-6 describes the PCC related signaling upon an IP-CAN session establishment.

In a roaming scenario the visited PCRF (V-PCRF) contacted by the BBERF/PCEF acts as a Diameter client and establishes a Diameter session towards the home PCRF (H-PCRF) over the S9 interface to get PCC rules from the user's home network before making the final authorization decision. These Diameter sessions stay alive as long as the UE is attached to the network maintaining the PDN connection.

In order to find and address the same PCRF the BBERF and PCEF provide the Diameter Routing Agent (DRA) of the PCRF realm with identity parameters upon the first interaction between the access entity and the PCRF realm, i.e. when establishing the Diameter sessions towards the PCRF. The identity parameters may comprise the user identity, the UE's IPv4 address and/or the UE's IPv6 prefix and PDN information.

Depending on the operator's configuration the routing towards the PCRF (i.e. the PCRF selection by the DRA) may be based either on the user identity or on the IPv4 address / IPv6 prefix [3GPP_TS_29.213]. When the user identity is used, all IP-CAN sessions of the UE use the same PCRF, and the PCRF can control the total usage of network resources by the UE. When the IPv4 address / IPv6 prefix is used, different IP-CAN sessions of the UE may use different PCRFs, and because there is no interaction between PCRFs in the same network, the PCRFs cannot control the total usage of network resources by the UE. The selected PCRF uses the identity information to associate the BBERF and PCEF related Diameter sessions of the same UE or IP-CAN session.

When an AF session is established, the application function AF acts as a Diameter client and establishes a Diameter session towards the PCRF over the Rx interface in order to send session information to the PCRF and to request the PCRF to report bearer level events taking place during the session. This Diameter session stays alive as long as the related AF session is active. Each AF session of the UE has an own Diameter session towards the PCRF. The AF may also establish a Diameter session with the PCRF to request a dedicated bearer for the AF session signaling. [3GPP_TS_29.214]

The PCRF correlates IP-CAN session level information exchanged with the PCEF via the Gx interface and the application level information obtained from the AF via the Rx based on the use of the user IPv4 address or IPv6 prefix. The UE and subscription identities may also be used in this session binding [3GPP_TS_29.213]. In case the UE identity in the IP-CAN level and the application level identity for the user are of different kinds (e.g. IMSI vs. IMS user identity not based on IMSI), the PCRF needs to

maintain, or have access to, the mapping between the identities [3GPP_TS_29.213]. Such mapping may be resolved in a standardized way within the user data convergence (UDC) work in Rel-10, by maintaining the identities in a common user data register accessible by relevant entities like PCRF.

When opening a Diameter session towards the PCRF, the AF provides the PCRF with AF session information which may comprise the UE IP address/prefix, user identification, service and media information, application identifier, charging identifier for charging correlation purposes, emergency traffic indication and a request for notifications of specific IP-CAN session events. The PCRF uses the information, possibly together with subscriber related information, for creating an authorization decision comprising authorized QoS and/or PCC/QoS rules and pushes the decision and other relevant information to the PCEF/BBERF, or waits for a request for the authorization before sending the authorization decision in the response, if the bearer control mode is UE only. A possible later AF session modification causes a similar message and parameter exchange between the AF and the PCRF to update the authorization. Figure A3-7 describes the PCC related signaling upon an AF session establishment, when the AF is the P-CSCF of IMS [3GPP_TS_29.214].

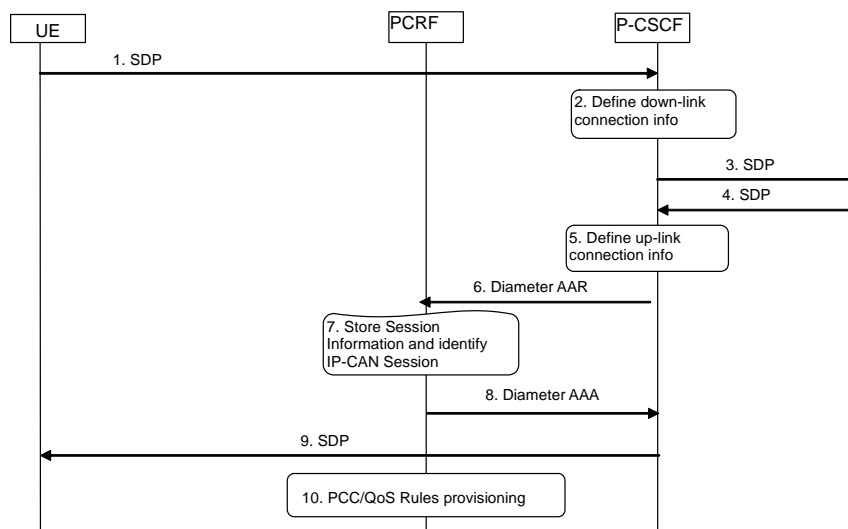


Figure A3-7: PCC related signaling upon an AF session establishment.

A PCC rule may comprise a service identifier (to identify the service or service component within the service data flow a PCC rule relates to), a service data flow description (IP addresses, ports, protocol, direction), a precedence value (to determine the order in which the service data flow templates are applied at service data flow detection in the PCEF), flow status (to define whether the service data flow is enabled or disabled), QoS parameters (i.e. the authorized QoS for the PCC rule), rating group / charging key, metering method (to indicate whether offline charging is metered by duration or volume or both), charging identifiers and reporting level (to define on which level the PCEF reports the usage for the related PCC rule). A QoS rule is a subset of a PCC rule, comprising a service data flow description, QoS parameters and precedence value. The PCRF sends PCC rules to the PCEF and QoS rules to the BBERF [3GPP_TS_29.212].

The authorized QoS provided by the PCRF in an authorization decision may refer to a PCC rule, to an IP-CAN bearer, to a QCI or to an access point name (APN). The authorized QoS information for a PCC rule may comprise a QCI, maximum bitrates (MBR) uplink and downlink, guaranteed bitrates (GBR) uplink and downlink and allocation/retention priority (ARP). The authorized QoS information for a default EPS bearer may comprise a QCI and allocation/retention priority (ARP). The provided QCI may only include values corresponding to non-guaranteed bit rates. The authorized QoS for a dedicated bearer may comprise a QCI, maximum bitrates (MBR) uplink and downlink, guaranteed bitrates (GBR) uplink and downlink and allocation/retention priority (ARP). The authorized QoS for a dedicated bearer is access specific, applicable to GPRS. The authorized QoS for QCI comprises an authorized maximum bit rate MBR per QCI. The authorized QoS for QCI applies only to IP-CAN types that support non-guaranteed bit rate (non-GBR) bearers that have a separate MBR (e.g. 3GPP-GPRS access). The authorized QoS for APN comprises an authorized aggregate maximum bit rate for the related APN. [3GPP_TS_29.212]

A modification to an existing authorization decision or to exchanged parameters may be caused by a request from the AF or PCEF/BBERF (including a resource modification request from the UE) or by a PCRF internal trigger. Depending on the source and on the bearer control mode, the PCRF either pushes a new decision to the PCRF/BBERF or waits for a request from the PCEF/BBERF and sends the new decision in the response.

2.3.3 Application detection and control

When there is no explicit service level signaling and hence no interaction between the application function AF and PCRF, the network may not be aware of the usage of such services by the UE even though the network may have defined policies related to the services. The user experience can be enhanced, if the network becomes aware of such services and the network is able to apply service specific policies.

3GPP solved this in Rel-11 with a traffic detection mechanisms based on deep packet inspection. 3GPP has standardized two architectural alternatives for the application detection and control: The TDF may be integrated with PCEF in the same gateway/entity or the TDF may be a stand-alone entity. The current Gx reference point and protocol is extended with TDF related parameters to support the integrated (PCEF + TDF) case. A new Sd reference point with a Diameter application protocol is defined between the PCRF and TDF for the standalone TDF case.

When solicited application reporting is applied, the PCRF informs the TDF, if allowed as per the user's privacy policies in the subscription profile, about the services that shall be detected. The TDF informs the PCRF, when a service start or stop has been detected. The PCRF defines PCC/QoS rules for the PCEF/BBERF and/or ADC rules for the TDF for the detected service and pushes an authorization decision with the rules to the PCEF/BBERF and/or TDF which enforces the policy on the SDF. If the TDF does not provide the PCRF with service data flow description(s) for the detected application, the TDF performs gating, redirection and bandwidth limitation for the detected application. If the TDF provides the PCRF with service data flow description(s) for the detected application, the enforcement actions resulting from the application detection may be performed by the PCEF, as part of the charging and policy enforcement per service data flow and by the BBERF for bearer binding, or may be performed by the TDF. When a standalone TDF is deployed and required to apply enforcement actions, the PCRF coordinates the operations with the PCC/QoS and ADC rules to ensure consistent service delivery.

When unsolicited application reporting is applied, the TDF is pre-configured on which applications to detect and report. Policy enforcement is performed by the PCEF. User profile configuration indicating whether application detection and control should be enabled is not required in this case.

2.3.4 Relevance for MEVICO WP4

Understanding the currently standardized 3GPP functionality for policy control is essential for discussing related enhancements in the scope of WP4.

In the 3GPP EPC, traffic steering to determine the QoS for traffic data flows is controlled by the Policy Control and Charging system. The PCC system implements operator-defined policies that can depend on user profiles and takes information about ongoing application traffic gained either from application level signaling (e.g. SIP for VoIP) and/or from extended packet inspection. PCC also supports different charging policies for different traffic data flows and allows limiting traffic bandwidths by dropping packets.

2.4 Voice Support in LTE

2.4.1 Overview

Voice and SMS over SAE can be supported via IMS or CS Core. An EPC network indicates to the UE that VoIP in LTE with IMS is supported with an "IMS voice over PS Session Supported Indication". This indicates to the UE that this serving area(s) (i.e. tracking area list) provides sufficient QoS and coverage for VoIP with IMS. Therefore, UE that has been provisioned with IMS VoIP with HPLMN can start IMS voice session based on this indication. Some EPC network may also support Single Radio Voice Call Continuity (SRVCC) feature [3GPP_TS_23.216] to improve voice coverage by handing over the voice session from LTE to 2/3G CS domain.

Some EPC networks may not support "IMS voice over PS Session Supported Indication" (e.g., spotty LTE coverage) and may want to rely on existing CS core for providing voice service. This can be done using the CS fallback (CSFB) feature as described in [3GPP_TS_23.272]. Basically, CSFB allows the UE to switch to 2/3G network from LTE in a controlled fashion for voice service usage.

2.4.2 IMS

2.4.2.1 Overall Architecture

Figure A3-8 depicts the network entities within the IMS and the reference points between them. Those network entities are described in the subsequent clauses.

The main IMS related 3GPP specifications are:

- The overall 3GPP network architecture, including IMS related network entities and interfaces, is specified in [3GPP_TS_23.002].
- A high-level (stage 2) procedural description of the IMS is provided in [3GPP_TS_23.228].
- Further stage 2 information on IMS call model and session handling is contained in [3GPP_TS_23.218].
- The main stage 3 specification of the IMS is in [3GPP_TS_24.229].

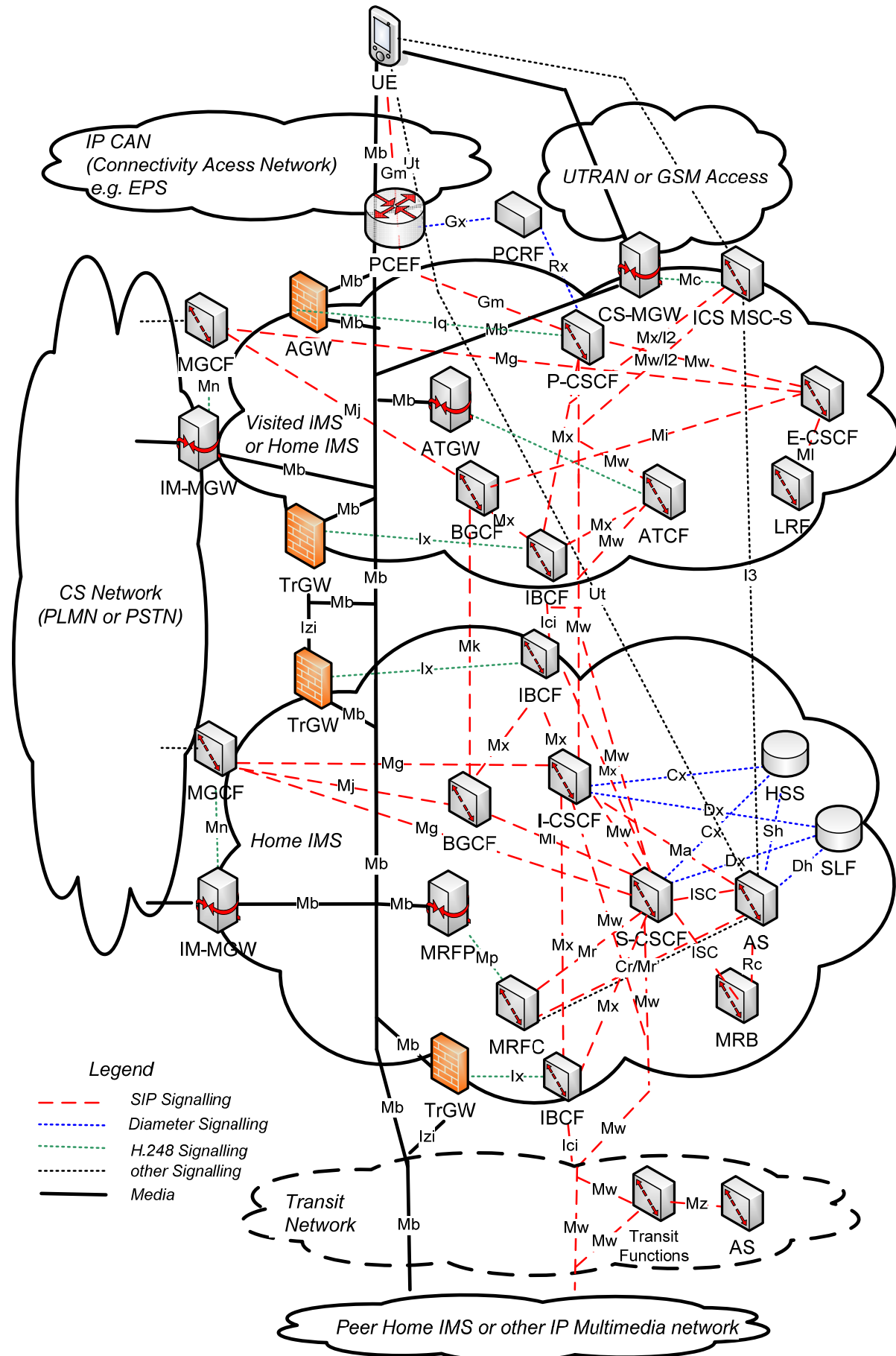


Figure A3-8: Configuration of IM Subsystem entities

2.4.2.2 Call Session Control Functions

A Call Session Control Functions (CSCF) is a SIP proxy ([RFC3261]) extended with special roles and functionality. CSCFs play a central role in the IMS call handling. Different types of CSCFs are defined that will be described in the following sections. Figure A3-9 depicts those different types of CSCFs in a simplified IMS architecture.

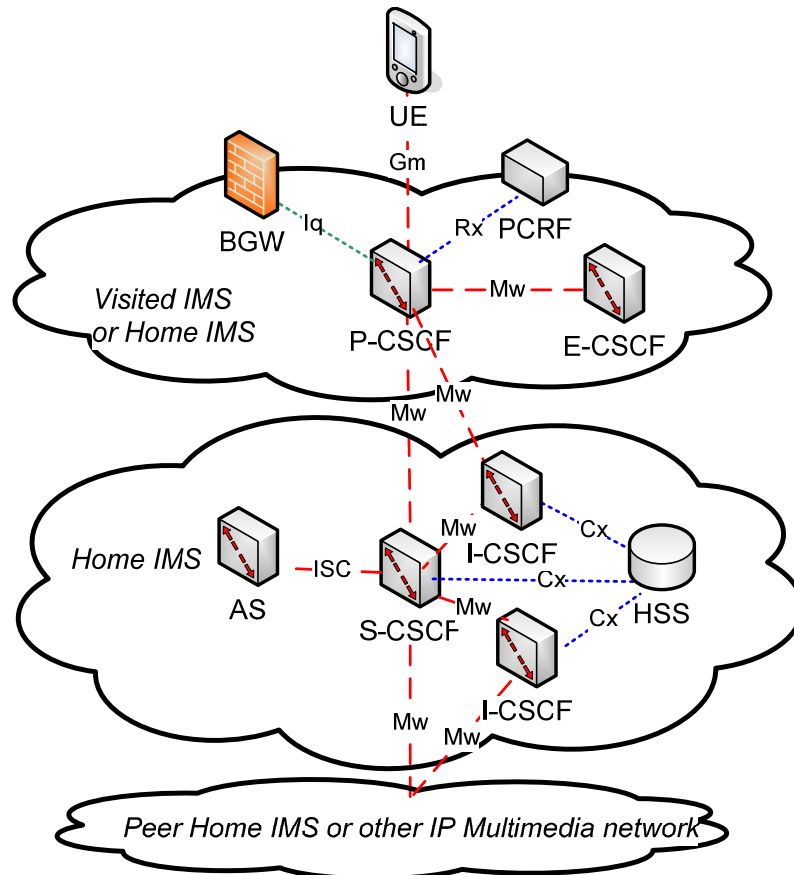


Figure A3-9: Call Session Control Functions in a simplified IMS architecture

Serving Call Session Control Function (S-CSCF)

The S-CSCF is the central IMS entity in the home IMS network.

The S-CSCF provides the following functions:

- SIP Registrar:
A user equipment (UE) registers within the IMS when it is switched on. At this point in time the S-CSCF is assigned to that UE, loads the corresponding IMS user profile from the Home Subscriber Server (HSS), and stores information related to the UE, such as the SIP signaling path towards that UE. A UE is registered at the S-CSCF is also termed "served UE"
- IMS User Authentication:
During the SIP registration, the S-CSCF interacts with a served UE to authenticate the user.
- Stores IMS User Profiles:
As long as a user is registered, the S-CSCF stores information related to that user.
- Session Control:
Each SIP session setup to establish media flows from or to a served UE will be routed through the S-CSCF assigned to that UE. The S-CSCF controls if the user is entitled for the desired session according to the policies of the operator, as described in the user profile. The S-CSCF may also adjust the session according to this policy.
- Service Control:
Special handling related to a particular service can be performed in an Application Server (AS). The S-CSCF can forward a SIP session setup to an application server for such service specific

treatment. The S-SCF is well suited for this task as it is located in the home network and home service control is an important IMS concept.

- Routing and Address Translation:
For a session setup originating from the served UE, the S-CSCF analyses the SIP request URI indicating the called party to determine the next SIP node where to send the request. The S-CSCF may also modify the Request URI and interact with external databases (such as ENUM) for that purpose.
For a terminating SIP session setup towards the served UE, the S-CSCF inserts stored routing information about the SIP signaling path towards the served UE.
- Charging Records:
The S-CSCF collect charging related information for ongoing SIP sessions.
- Lawful Interception Support:
- Privacy Support:
When the S-CSCF forwards SIP messages to un-trusted SIP peers, it will remove protected information such as the identity of the calling party

Proxy Call Session Control Function (P-CSCF)

The P-CSCF is the outmost SIP-level entity toward a served UE. If IMS roaming is used the P-CSCF is the central IMS entity in the visited IMS network. Otherwise, the P-CSCF is also located in the home network.

When a UE registers, it is assigned a P-CSCF as entry point towards the IMS. The P-CSCF stores information related to that served UE while it remains registered and forwards any SIP message to or from the served UE.

The P-CSCF provides the following functions:

- Integrity and Confidentiality:
The P-CSCF protects the integrity and confidentiality of SIP messages at the Gm interface towards the served UE.
- SIP Header Compression:
The P-CSCF may serve as endpoint of SIP header compression at the Gm interface towards the served UE.
- Charging Records:
The P-CSCF collect charging related information for ongoing SIP sessions as required in the visited network.
- Policy and Charging Control (PCC) Support:
The P-CSCF may provide information about ongoing services negotiated via SIP towards the Policy and Charging Resource Function (PCRF).
- Support for Traversal of Customer Premise Equipment (CPE):
The P-CSCF supports procedures to enable the traversal of SIP signalling through a CPE. Furthermore, it can configure an access gateway (AGW) to enable the traversal of media flows through the CPE.
- SIP Application Level Gateway (SIP-ALG):
The P-CSCF supports the control of an access gateway (AGW) acting as a NAT and firewall for media flows, and modifies the media related address information within SIP/SDP accordingly
- Lawful Interception Support
- Support of Emergency Calls:
The P-CSCF recognizes emergency calls and routes them to an Emergency CSCF.

Interrogating Call Session Control Function (I-CSCF)

When receiving a SIP message for a user, the I-CSCF is used to look up the S-CSCF serving that user in the Home Subscriber Server (HSS), and then forward the SIP message to that S-CSCF. The I-CSCF does not need to store any user related data and does not need to stay in the path for subsequent SIP messages.

The I-CSCF is both used when a UE registers to the network and when a session setup destined for a served user is received in a home IMS, e.g. from some peer IMS network or from the PSTN.

Emergency Call Session Control Function (E-CSCF)

The E-CSCF handles emergency calls and looks up location information about the callee from the Location Retrieval Function (LRF) and forwards the call to a Public Safety Answering Point (PSAP) or emergency center.

2.4.2.3 Subscriber Databases

Figure A3-10 shows the Subscriber Databases and their interfaces towards other nodes in the IMS. Diameter is used as signaling protocol on those interfaces.

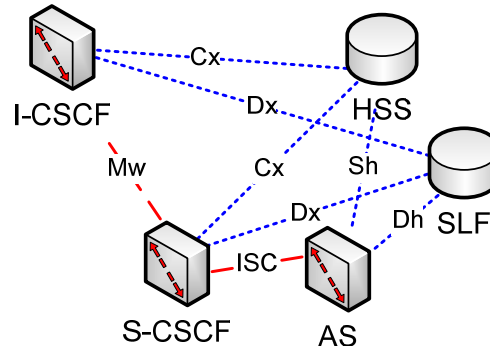


Figure A3-10: Subscriber Databases and their interfaces

The protocol on the interfaces to subscriber databases is based on Diameter, [RFC3588].

Home Subscriber Server (HSS)

The HSS is located in the home network of a given user and is the master database for that user, containing both subscription-related information and location related information related to that user:

- User Identification, Numbering and addressing information;
- User Security information: Network access control information for authentication and authorization;
- User Location information at inter-system level: the HSS supports the user registration, and stores inter-system location information;
- User profile information.

The HSS provides support to the call control servers for:

- authentication and authorization,
- routing/roaming procedures by solving naming/addressing resolution, and providing location information, and
- provisioning of subscription related information.

The HSS contains data related to all domains and subsystems defined by 3GPP (CS domain, GPRS, EPS, and IMS).

A Home Network may contain one or several HSSs.

Subscription Locator Function (SLF)

If a home network contains several HSSes, the SLF is queried by CSCFs and ASes to look up the HSS containing the subscriber specific data of a given subscriber.

2.4.2.4 Application Server (AS)

IMS is designed as generic service delivery platform. This means that the IMS core is agnostic with regards to the service and not all services are fully standardized. An Application Server (AS) offers value added IM services and resides either in the user's home network or in a third party location.

Figure A3-11 shows an Application server and its most important interface. Certain types of application servers can have additional interface.

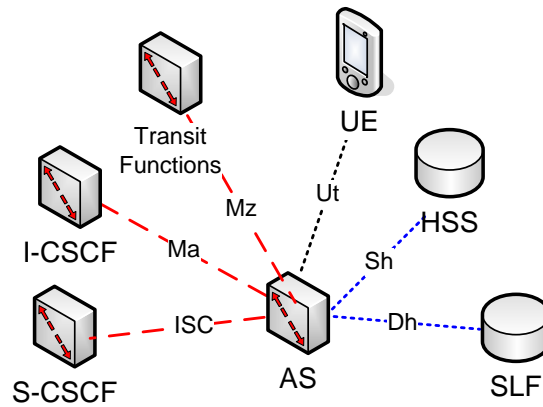


Figure A3-11: The Application Server and its interfaces

Service specific SIP processing is performed in Application Servers connected via ISC interface to the IMS core. The internal behavior of AS is not fully standardized, but the IMS service control (ISC) Interface towards the AS is standardized. The S-CSCF decide whether to invoke ASes to treat SIP messages, applying so-called "initial Filter Criteria" (iFC) stored in a subscriber profile.

For the configuration of services, an AS may provide the Ut interface towards the user equipment.

The AS may access or modify service specific content stored in a user profile in the HSS.

While not every AS is standardized, a number of different AS types have been standardized, for instance:

- The Telephony Application Server (TAS)
This AS is responsible to handle MMTEL supplementary services..
- The Service Centralization and Continuity Application Server (SCC AS)
This AS plays a central role for ICS.
- Media Resource Control Application Server
An AS that interacts, or is combined with, an MRFC can play a role in conference control.
- Presence Application Server (Standardized by the Open mobile Alliance, OMA)
- Push-to-talk over Cellular (PoC) Application Server (Standardized by the Open mobile Alliance, OMA)
- Instant Messaging (IM) Application Server (Standardized by the Open mobile Alliance, OMA)
- IP-SM-GW:
This AS provides messaging interworking services.
- OSA service capability server (OSA SCS):
This AS provides interworking to the OSA framework Application Server and thus also provides a standardized way for third party secure access to the IM subsystem.
- IP Multimedia Service Switching Function (IM-SSF):
This AS hosts CAMEL network features (i.e. trigger detection points, CAMEL Service Switching Finite State Machine, etc) and provides interworking to CAP.

2.4.2.5 Entities related to the Interworking with Circuit Switched Networks

Figure A3-12 depicts network entities that are affected by the interworking with circuit switched networks.

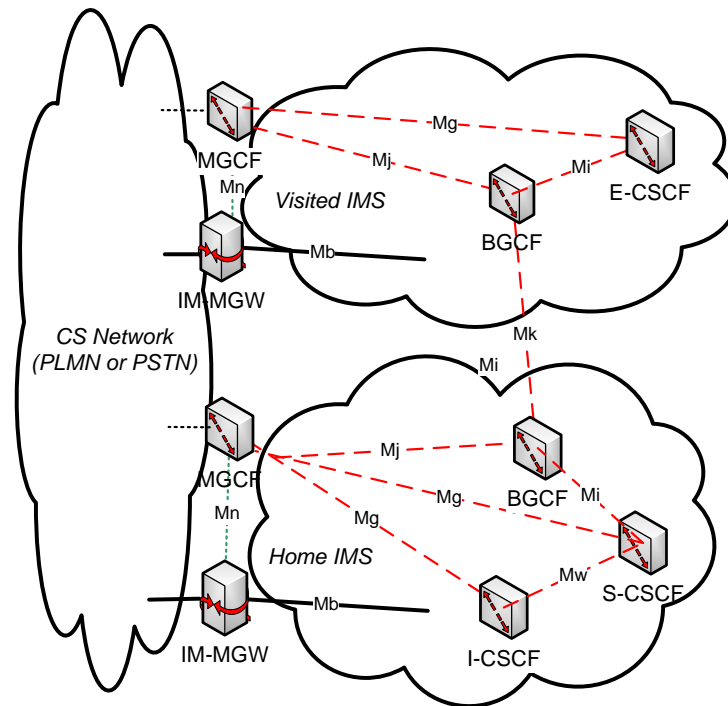


Figure A3-12: Entities related to the Interworking with Circuit Switched Networks

Media Gateway Control Function (MGCF)

The MGCF provides a conversion between SIP signaling, as used in the IMS, and signaling used in circuit switched networks (ISUP, BICC, SIP-I), and controls the attached IM-MGW.

IP Multimedia Media Gateway (IM-MGW)

The IM-MGW provides transport conversion between the transport used in the CS network, for instance the Nb framing protocol or TDM transport, and the RTP/UDP/IP media transport used in the IMS. In addition, the IM-MGW can be configured to transcode media.

Breakout Gateway Control Function (BGCF)

If a call needs to be routed to the PSTN, the S-CSCF forwards the call to a BGCF. The BGCF analyses the called number, selects a suitable MGCF, and forwards the call to that MGCF.

Instead of directly forwarding a call to a MGCF, a BGCF can decide to forward a call to a BGCF in another network that will then forward the call to an MGCF.

The BGCF does not need to store any user related data and does not need to stay in the path for subsequent SIP messages.

2.4.2.6 Media Processing Resources

The media processing resources described in this section can serve as Conference Bridge for a multi-party conference, as trans-coding device, and as source for tones or announcements. The functionality is distributed over several network entities, as depicted in figure A3-13.

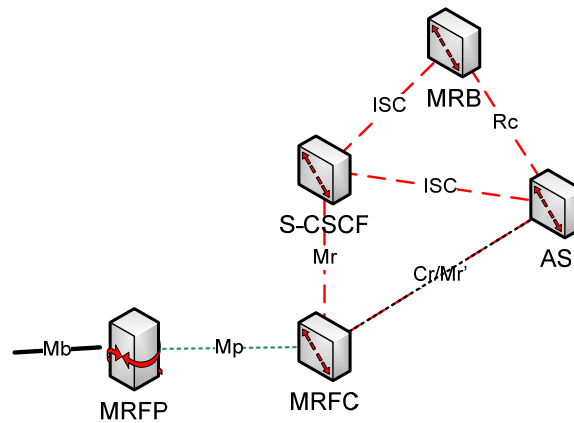


Figure A3-13: Media Processing Resources in the IMS

Media Resource Control Application Server (AS)

An AS may fulfill several Media Resource Control related Functions:

- The AS may analyze codec information in SIP requests to determine if trans-coding is required and then invoke the MRFC.
- The AS may perform conference booking and management of booking information
- When processing SIP requests, the AS may determine that tones or announcements are required and then invoke the MRFC.

The AS may communicate with the MRFC using SIP either via the ISC interface, the S-CSCF and the Mr interface, or directly via the Mr' interface. In addition, it can perform media control via the Cr interface.

However, some of the related interactions are not specified in great detail, as the AS and MRFC are frequently combined.

Media Resource Function Controller (MRFC)

The MRFC is either invoked by an AS or directly by the S-CSCF.

It analyses SIP signaling and possible additional information from the AS to determine the required media functions, configures the MRFP accordingly and collects media processing related charging information.

Media Resource Function Processor (MRFP)

Upon request from the MRFC, the MRFP performs a subset of the processing of media flows. The MRFC may:

- mix incoming media streams from multiple parties and perform related floor control,
- forward media streams to multiple destinations,
- transcode media streams, and
- generate media streams with tones and announcements

Media Resource Broker (MRB)

The MRB supports the sharing of a pool of heterogeneous MRF resources by multiple heterogeneous applications. The MRB assigns (and later releases) specific suitable MRF resources to calls when being addressed by S-CSCF or AS.

2.4.2.7 Entities at the NNI between IMS networks

At the border of an IMS network, either at an interconnection towards another IMS networks, or towards some other IP multimedia network, an IBCF, possibly with attached TrGW, may optionally be deployed. IBCF may be deployed at an interface that interconnects two home IMSes, as well as at an interface that interconnects a visited IMS and a home IMS. This is depicted in figure A3-14 below.

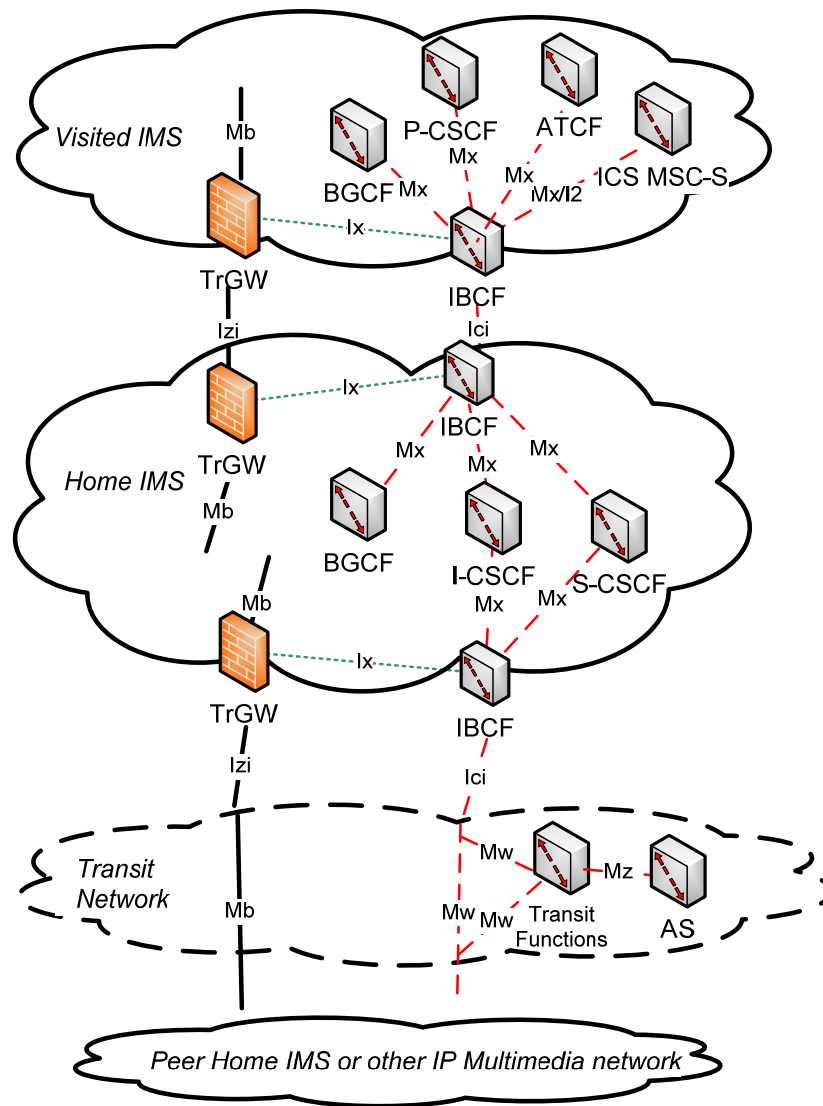


Figure A3-14: Entities at the NNI border of IMS networks

Interconnection Border Control Function (IBCF)

The IBCF performs functions related to the protection of an IMS network, to address translation, and IP version interworking. The IBCF may:

- screen SIP signalling, e.g. to remove unsupported SIP headers,
- hide the topology of the IMS network by replacing related address information within SIP with opaque tokens,
- act as an SIP Application Level Gateway (ALG) that inserts of a transition gateway (TrGW) acting as a NAT and firewall for media flows, and modify the media related address information within SIP/SDP accordingly, and
- configure the TrGW to transcode and update the media information within SIP/SDP accordingly.

Transition Gateway (TrGW)

Upon request from the IBCF, the TrGW opens pinholes that allow media streams to enter or leave the IMS, and thus acts as a kind of firewall to protect the IMS network.

The TrGW acts as NAT and converts IP addresses and ports of any IP packet it passes. This enables the usage of private address spaces within the IMS, and also enables interworking between IPv4 and IPv6.

A TrGW may also support the transcoding of media.

Transit Functions

The IMS Transit Functions perform an analysis of the destination address, and determine where to route the session. The session may be routed directly to an MGCF, BGCF, or to another IMS entity in the same network, to another IMS network, or to a CS domain or PSTN.

The IMS Transit Functions might reside in a stand-alone entity or might be combined with the functionality of an MGCF, a BGCF, an I-CSCF, an S-CSCF or an IBCF.

When IMS provides transit functionality to other network operators or enterprise networks, the IMS may also provide IMS applications services to the network operator or enterprise network. The Transit function then invokes an AS via the Mz interface based on local configured filter criteria.

2.4.2.8 IMS Entities at the Border towards Access Networks

The IMS entities at the border towards Access Networks and their surrounding networks are depicted in figure A3-15 below.

Some so-called IP connectivity access network (IP-CAN) is used to provide a connection between UE and IMS, for instance a GPRS or EPS network, or a DSL access network, or some other IP access network.

Some access networks such as GPRS or EPS provide a point-to-point connection that tunnels IP towards the UE. Such a point-to-point connection is termed an IP-CAN bearer. The Policy and Charging Control (PCC) system including the Policy and Charging Resource Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) can be used to configure such IP-CAN bearers. A simple variant of the PCC architecture is depicted in figure A3-15, but additional variants exist for SAE.

A UE can be located behind a so-called Customer Premise Equipment (CPE) that is the entry point to the customer's private network. A set top box terminating DSL in the customer's home is an example of such a CPE. A CPE acts as a network address translator (NAT) and firewall and modifies the IP addresses and port information of all IP packets that traverse it, including both packets to transport SIP signalling and media flows. If a CPE is deployed, the IMS needs to support the traversal of media flows through the CPE. Two options are standardized:

- An AGW as described below is used.
- The Interactive Connectivity Establishment (ICE), IETF RFC 5245 [RFC5254], is used by the UE. To support ICE, a STUN server and/or STUN proxy according to IETF RFC 5389 [RFC5389] is required within the network.

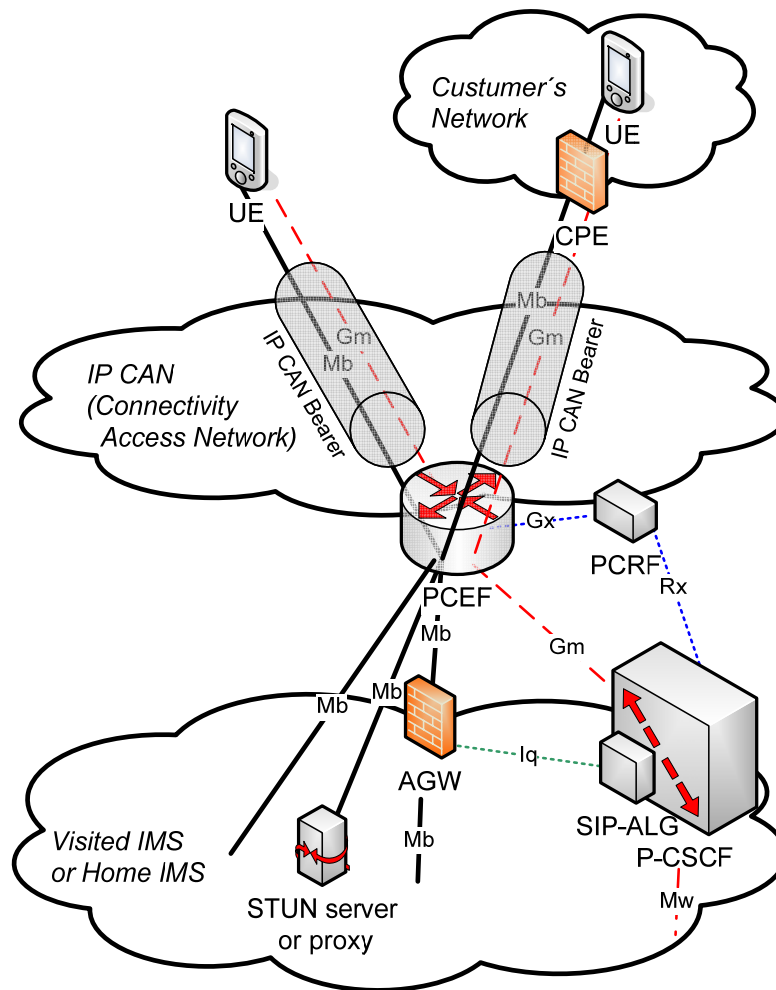


Figure A3-15: Entities at the border of IMS networks towards access networks

The P-CSCF, PCEF, and PCRF have already been described.

Access Gateway (AGW)

Upon request from the SIP-ALG within the P-CSCF, the AGW opens pinholes that allow media streams to enter or leave the IMS, and thus acts as a kind of firewall to protect the IMS network.

The AGW acts as NAT and converts IP addresses and ports of any IP packet it passes. This enables the usage of private address spaces within the IMS, and also enables interworking between IPv4 and IPv6.

To enable the traversal of a CPE, the AGW may be configured to apply latching: The AGW will then send packets of an IP flow towards the UE to the IP address and port number that was indicated as source in corresponding IP packets received from the UE.

2.4.2.9 Entities to support IMS Centralized Services and Service Continuity

3GPP has worked on features that ease a transition from existing voice services in the CS domain to the IMS over several releases. The significant milestones within these developments were:

- Rel-8 Service Continuity (SC) [3GPP_TS_23.237] provides general continuity of all kind of IMS sessions, not restricted to bi-directional speech calls only.
- Rel-8 IMS Centralized Services (ICS) [3GPP_TS_23.292] enables all telephony services to be centralized in the IMS, i.e. CS services are replaced by equivalent IMS services.
- Service Continuity (SC) and IMS Centralized Services (ICS) use a common network architecture and can be seen as one functional package.
- In Rel-8 Single Radio VCC (SR-VCC) has been developed to overcome the dual radio requirement for voice session transfers.

- In Rel-9 terminated access domain selection (T-ADS) has been specified to avoid routing of IMS calls towards non VoIP capable access types. The HSS is queried about the UE's network voice capabilities when a voice call is received and the HSS in turn pulls this information from the SGSB or MME.
- In Rel-10 Single Radio VCC (SR-VCC) has been enhanced (called eSRVCC) to allow voice media anchoring and session transfer at the service PLMN to improve user experience during SRVCC (i.e. minimize voice gap).

Entities to support IMS Centralized Services and Service Continuity are depicted in figure A3-16.

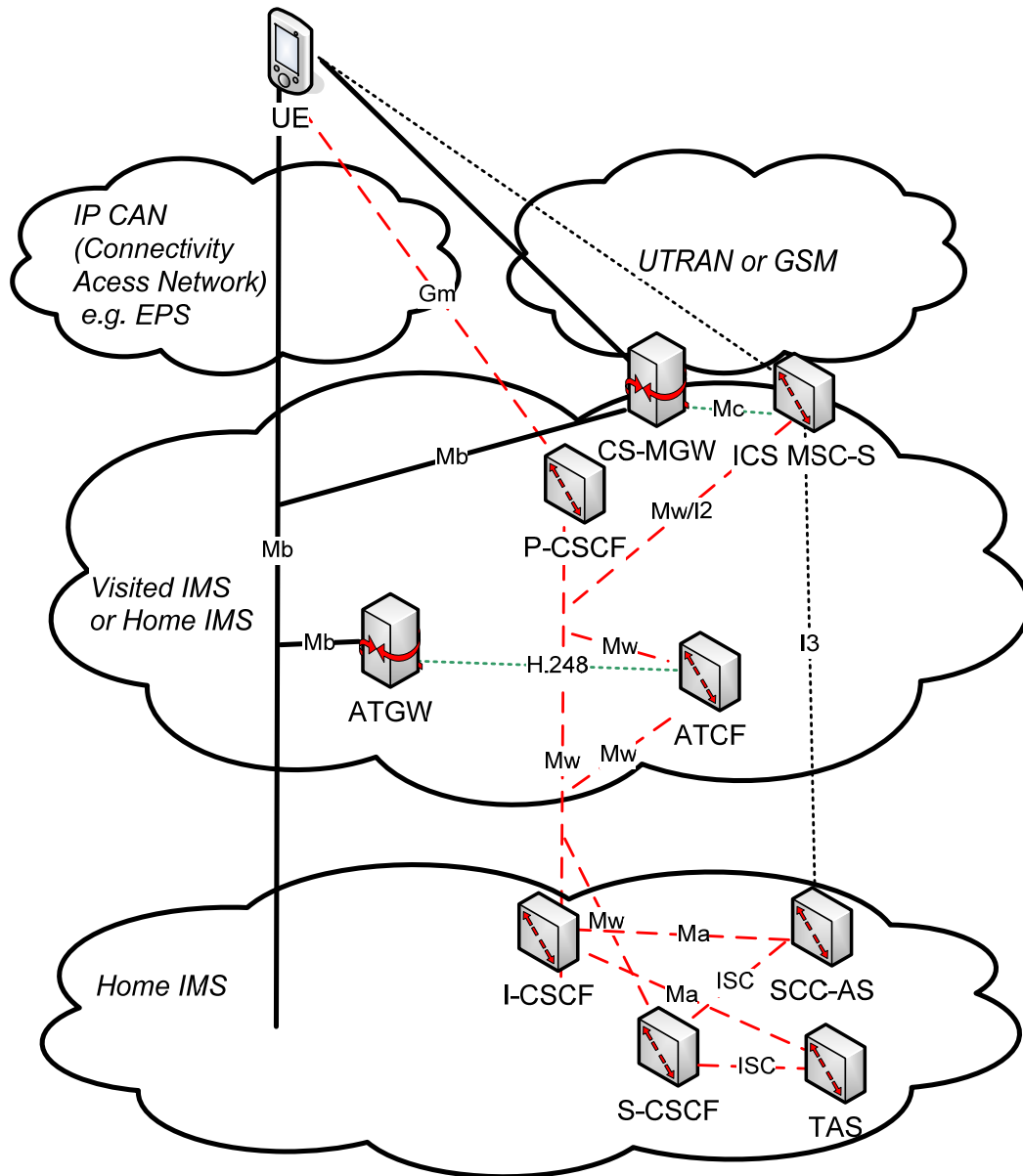


Figure A3-16: Entities to support IMS Centralized Services and Service Continuity

MSC server enhanced for ICS and Circuit switched Media Gateway (CS-MGW)

An MSC Server may be enhanced with ICS specific functions. In addition to the standard MSC Server functionality an enhanced MSC Server performs inter-working between the user-network signalling on the CS access and IMS SIP.

It also controls a CS- MGW that provides inter-working between CS bearers and RTP bearers used in the IMS.

For the support of Service Continuity only, an MSC Server does not need to provide ICS capabilities. As an example, an MSC server can be enhanced for SRVCC without support of ICS.

Service Centralization and Continuity Application Server (SCC AS),

The SCC AS is a home network based IMS Application that provides specific functionality to IMS Service Centralization (ICS) and Service Continuity (SC).

The SCC AS provides SIP UA behavior on behalf of the UE for setup and control of for IMS sessions using CS bearers. The SCC AS combines the service control signaling with the description of the bearer (e.g. SDP when using Gm) with the service control via the CS access and presents this as standard IMS session on behalf of the UE to the sub-sequent application servers and the remote end.

The SCC AS performs Terminating Access Domain Selection (T-ADS) to direct an incoming session to an ICS User. This is performed by selecting one of the registered contacts or by performing a breakout to the CS domain.

Access Transfer Control Function (ATCF) and Access Transfer Gateway (ATGW)

The ATCF and ATGW are optional function in the serving (visited if roaming) network.

When SRVCC enhanced with ATCF is used, the ATCF is included in the session control plane for the duration of the call before and after Access Transfer. The ATCF perform the Access Transfer and update the ATGW with the new media path for the (CS) access leg,

The ATGW is controlled by the ATCF and, if SRVCC enhanced with ATCF is used, stays in the session media path for the duration of the call and, based on the local policy, after Access Transfer to avoid updating the remote leg. It also supports transcoding after SRVCC handover in case the media that was used prior to the handover is not supported by the MSC server.

It is recommended that the ATCF and ATGW are co-located with one of the existing functional entities within the serving network (ATCF with P-CSCF, IBCF, or MSC Server; ATGW with AGW, TrGW, or CS-MGW).

2.4.3 CS Fallback

To support voice service in EPC with CS Fallback (CSFB) feature, the network must be able to page the UE for CS terminating call invocation, to process the request from UE for Mobile Originated (MO) CS, and to instruct the UE to switch over to 2G/3G to continue the voice service processed within CS Core.

Besides voice, CS fallback in EPS also applies for other CS-domain services by reuse of CS infrastructure when UE is served by E-UTRAN. CSFB is applicable only when E-UTRAN coverage overlaps with 2G/3G coverage. The following figure shows the architecture for CSFB in the EPC-3GPP environment.

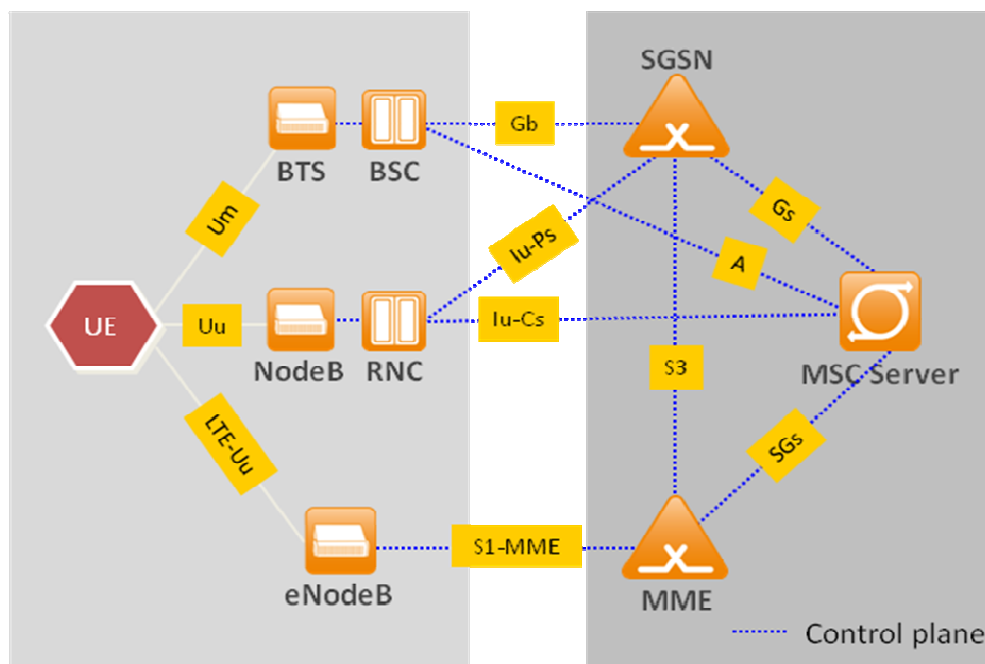


Figure A3-17: CS fallback architecture

The SGs interface plays the main role for CSFB because it allows the UE to perform IMSI attach to the Mobile Switching Center (MSC) and also allows the MSC to page the UE for CS terminating calls.

S3 interface is only needed in CSFB when ISR is applied in the network. It allows the paging message from the MSC to be forwarded to the 2G/3G PS network via MME when ISR is active. Without it, the UE which has reselected to 2G/3G during idle mode will not be able to respond to a CS-MT page request that is sent over the SGs interface by the MSC.

In order for the UE to use CSFB, the UE first performs a combined EPS/IMSI attach procedure (or combined TAU). This allows the MME to perform location update procedure via the SGs interface to a MSC. MME selects the MSC based on the current UE location. The idea is that the selected MSC is also serving the overlapping 2G/3G access. After the MSC performed the IMSI attach, the CS domain parameters (TMSI, LAI) are passed back to UE via SGs and the existence of these CS parameters indicate to the UE that the combined attach/TAU was successful.

When UE wants to initiate a voice call, it sends Service Request (EXTENDED SERVICE REQUEST message) with CSFB Indicator to the MME. Based on this indication MME initiates S1-AP Initial Context Setup procedure including CSFB Indicator towards E-UTRAN, which initiates mobility procedure towards GSM or UMTS. The mobility procedure can be PS-Handover, Cell Change Order (with or without NACC), or RRC connection release with redirection info. It is the decision of E-UTRAN which mobility procedure to invoke. For CS emergency call with CSFB, the UE also includes an emergency indicator in the Extended Service request message in addition to the CSFB indicator. This emergency indicator allows the MME and E-UTRAN to apply special handling if needed.

In mobile terminating call case, MME receives paging message over SGs interface from MSC. MME finds out the correct S-TMSI based on TMSI (or IMSI), included in the paging message received over SGs interface, and carries out paging of the UE. The paging message sent to UE includes CS domain indicator indicating CS domain.

The reception of CS domain indicator triggers the UE to send Service Request (EXTENDED SERVICE REQUEST) message including CSFB Indicator to MME. Based on this information, MME initiates S1-AP Initial Context Setup procedure including CSFB Indicator towards E-UTRAN. The mobility procedure is described in the mobility-originated scenario above.

Once the UE is tuned to 2G/3G, it continues with the LAI check and then MO/MT call setup procedure via the existing procedures defined in CS domain.

After the CS call is ended, the UE may return back to E-UTRAN based on the cell selection criteria/mechanism in the serving network.

During the CSFB procedure, the UE may select a 2G/3G cell which may result in performing LAU procedure prior to the MO/MT signalling. This LAU adds delay to the overall call setup time. To minimize this delay, a few performance enhancements are added to Release 9. This includes:

- The possibility for the MSC to be configured to lower the frequency of Authentication, TMSI reallocation and Identity check for UEs that are EPS/IMSI attached via the SGs interface,
- “System information for multiple cells” is included in the RRC connection release with redirection info message. This allows the UE to access the target cell without acquiring all the system information.
- In NMO I a CSFB UE may perform separate LAU with “follow-on request” flag and RAU procedures instead of a Combined RA/LA Update procedure to speed up the CSFB procedure. This allows the MSC to continue with the same signalling connection for CS MO call setup.
- 2G/3G biased idle mode camping policy so that UE are mostly camped in 2G/3G during idle mode. This minimizes the number of occurrences of CSFB as the UE are starting usually from 2G/3G.

2.4.4 Single Radio Voice Call Continuity

Single Radio Voice Call Continuity (SR-VCC), as specified in [3GPP_TS_23.216], enables the operator to extend the LTE's IMS VoIP coverage by defining handover mechanism from LTE to 2G/3G radio access with CS domain. The voice handling mechanism requires the bearer level handover procedures between the Evolved Packet Core and Circuit-Switched Core (i.e., MSC) and access legs domain switching function between IMS and CS as specified in 3GPP [3GPP_TS_23.237]. The non-voice component (e.g., video streaming, file transfer, etc) can be handled in conjunction with SR-VCC based on Inter-RAT PS procedures as specified in [3GPP_TS_23.401].

The highlight part in the following figure shows where the IMS Service Continuity procedure is started within the overall SRVCC procedure. Other parts within this figure are related to bearer handover aspects.

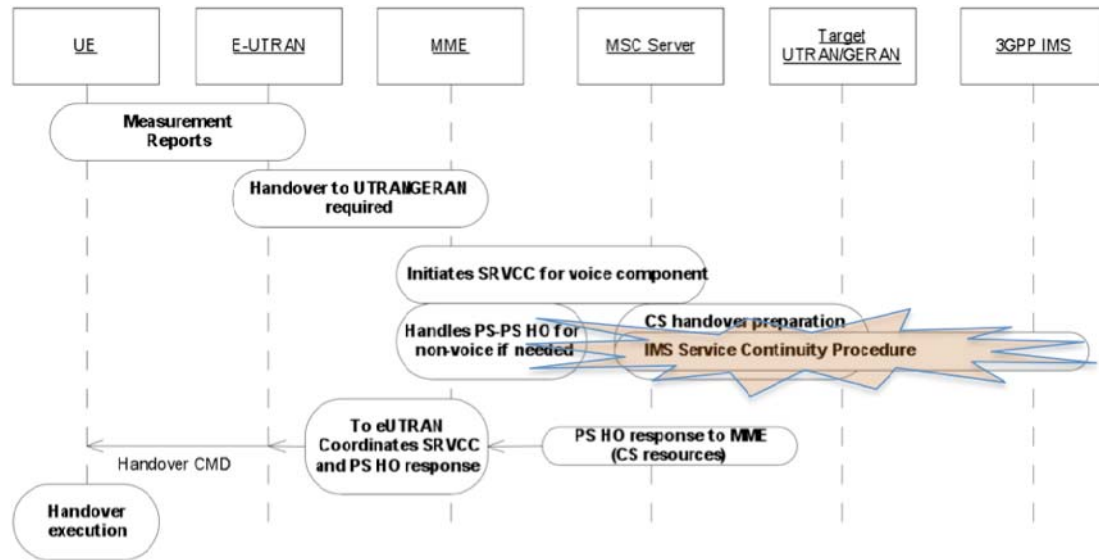


Figure A3-18: Overall high level procedure for SRVCC

The MME and MSC server enhanced for SRVCC is connected via Sv interface (see [3GPP_TS_23.216]). When SRVCC handover is needed, E-UTRAN sends an indication to MME. E-UTRAN determines whether this is just a PS to CS handover or both PS to CS and PS to PS handover to the target cell. This information is given to MME as part of the handover required message.

MME then initiates the PS-CS handover with the MSC via the Sv interface. MSC performs the CS handover procedure with the target cell (target cell ID is sent via Sv) via the existing CS handover procedures. If PS to PS handover is also required, the MME starts the inter RAT PS handover procedure as defined in [3GPP_TS_23.401] with PS voice bearer context marked so that the target network will not allocate PS resources for that context as it has been transferred to the CS Domain.

When the target network has successfully allocated the resources, the handover command is sent back to the source (i.e. to the MME) via MSC and Sv interface. MME forwards this handover command to E-UTRAN which ends in the UE. UE then tunes to target network based on this handover command. At this point, UE switches the PS voice to CS voice locally.

2.4.5 Relevance for MEVICO WP4

The access network selection, as studied by MEVICO WP4, is in 3GPP handled by special voice call related functionality:

Whereas previous 3GPP radio technologies (GERAN and UTRAN/HSPA) featured a dedicated "circuit-switched domain" to support circuit switched connections that are primarily used for voice traffic, LTE does only provide IP connectivity and relies upon VoIP. Considerable effort was spent in 3GPP to support a migration to LTE with continued voice support. It is assumed that parallel coverage with different radio technologies will be available soon, possibly with some areas not having LTE coverage for a while.

3GPP solutions allow that terminals camping in LTE, with or without an active data session, are being transferred to pre-LTE radio networks once a voice call needs to be set up (CS fallback), i.e. traffic steering is based on presence/absence of voice calls. Due to limitations of terminals that do not support simultaneous connectivity over several radio networks, data traffic are handed over to a different radio technology together with voice traffic.

3GPP also supports a seamless handover of voice calls between radio networks and between VoIP and circuit switched voice traffic to be applied when a UE moves out of, or into LTE coverage ("Voice Call Continuity"), i.e. a special traffic steering for voice calls based on LTE radio coverage.

To support VoIP, 3GPP has defined the IMS, which is involved in CS fallback and VCC (Single Radio and Dual Radio VCC) and designed to provide the same services as circuit switched voice. Within the IMS, the Service Centralization and Continuity Application Server (SCC AS), plays a central role for those purposes: Among other tasks, the SCC AS performs Terminating Access Domain Selection (T-ADS) to direct an incoming call to a terminal either via CS access or as VoIP calls via LTE or HSPA access dependent on access capabilities and user/operator preferences.

In addition, the IMS is tightly integrated within the PCC system, which allows that traffic related to services negotiated via the IMS is assigned to bearers with appropriate QoS for their requirements. This functionality affects WP4.

2.5 Traffic Offloading to WLAN

Basic 3GPP WLAN Interworking is specified in [3GPP_TS_23.234].

2.5.1 Offload per PDN Connection

In 3GPP Rel-8 specifications it is assumed that the UE uses a single (either a 3GPP or a non-3GPP) access network for all of its PDN connections; In Rel-10 the specifications are enhanced to allow that different PDN connections use different access networks as depicted in figure A3-19. Moreover PDN connections can be handed over independently between the access networks if the UE is connected to a 3GPP and a non-3GPP access network with the limitation that PDN connections to a given APN shall use the same access network. (Note the UE cannot use more than one 3GPP radio technology (E-UTRAN or UTRAN or GERAN) simultaneously.)

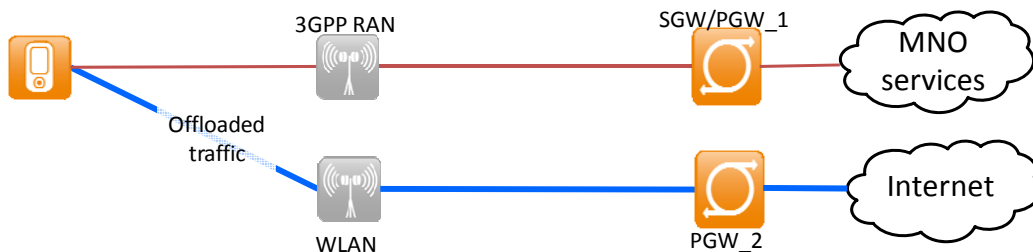


Figure A3-19: PDN connection based mobility

This solution enables a PDN connection level offloading, e.g., the PDN connection to access the Internet can be moved to WLAN when it is available, but the PDN connection to access special operator services (e.g., IMS) can be kept in 3GPP. In this way traffic can be offloaded from the 3GPP radio, but no core network resources are saved. In order to enable operator control for the selection of access networks for different PDN connections ANDSF is enhanced with inter-system routing policies that can be used by UEs to select appropriate access networks for its PDN connections.

2.5.2 IP Flow Mobility and Seamless WLAN Offload

Another extension of the non-3GPP interworking architecture is provided by flow based mobility between 3GPP and non-3GPP access networks. With this feature it is possible to select and change access networks (e.g., WLAN or 3GPP access like LTE) dynamically for IP flows without the need to change the IP address, which means the change of the access technology is transparent to the applications. E.g., a UE can use 3GPP access for Web services in general and can start using an available WLAN when downloading a large file. As a prerequisite the terminal must be multi-radio capable. In this way some flows can use an available non-3GPP access network like a WiFi hotspot instead of a 3GPP radio technology to access operator services via the mobile core network. Although non-3GPP access technologies may be used for certain services all traffic is still routed through the operator's packet core. This results in unloading the radio network without significant impact to the core network load. Routing all traffic through the EPC enables the operator to control the data traffic (policing, QoS control, charging).

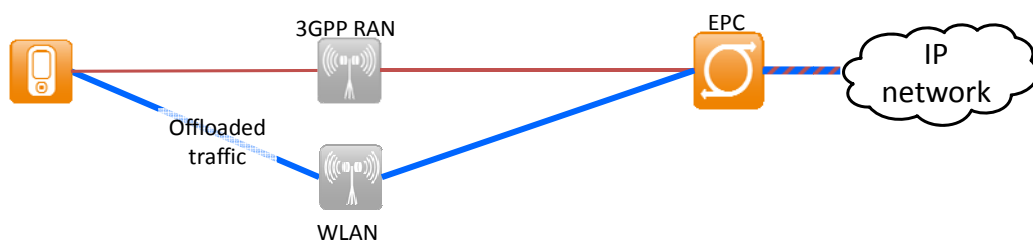


Figure A3-20: Flow based mobility

A DSMIPv6 based solution is part of 3GPP Rel-10 specifications [3GPP_TS_23.261] [3GPP_TS_23.327]. When a UE configures different IP addresses on multiple accesses it registers these

addresses with the DSMIPv6 Home Agent (HA) located in the P-GW as care-of-addresses (CoA). In order to route IP flows through a specific access network the UE requests storing appropriate routing filters for that access at the HA side. This is done within the DSMIPv6 signalling using the Flow Identification (FID) mobility option of DSMIPv6. The FID option defines a routing rule which contains a routing filter and a routing address. To install/remove/move an IP flow the UE creates a new IP flow binding or removes/updates the IP flow binding at the HA by using DSMIPv6 signalling. This can happen any time during a session.

In order to enable operator control for the selection of access networks for different flows ANDSF is enhanced with inter-system routing policies that can be used by UEs to select appropriate access networks for specific IP flows.

2.5.3 Non-Seamless WLAN offload

Non-seamless WLAN offload is a simple mechanism for the UE to use a non-3GPP access network when it is available, while changing automatically or manually to 3GPP access when needed. However, this kind of offload is not transparent to the applications. The benefit of non-seamless WLAN offload is that it totally saves 3GPP network resources (in the RAN and CN). As a consequence the operator cannot provide any 3GPP based service for offloaded traffic anymore and mobility is also not supported by the network. This type of offloading is already available and used today depending on the capability of the UE and applications. As a prerequisite the terminal must be multi-radio capable. As most of the current applications can survive a short break in the connection and change of IP address when the UE changes the access network, non-seamless WLAN offload is sufficient for non-real-time IP services, such as Web browsing or email access.

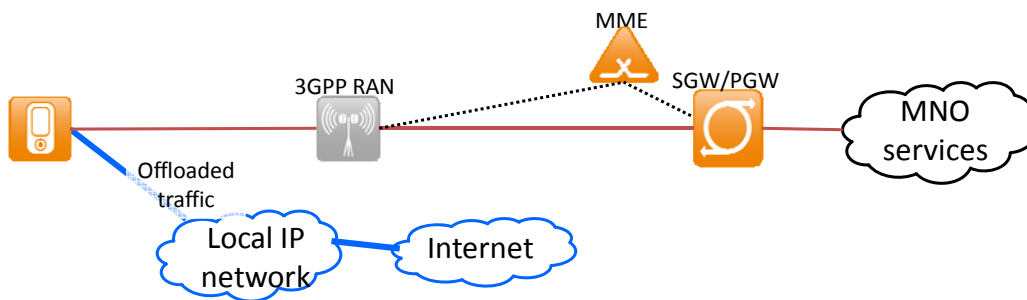


Figure A3-21: Non-seamless WLAN offload

A solution using ANDSF is specified in [3GPP_TS_23.402] where an operator can provide inter-system routing policies to the UE to determine when to use an available WLAN instead of 3GPP radio access for non-seamless WLAN offload.

2.5.4 The Access Network Discovery and Selection Function (ANDSF)

The Access Network Discovery and Selection Function (ANDSF) provide the user's device with information (called ANDSF rules) to enable for inter-system mobility, inter-system routing and access network discovery. This information allows the UE to select the most preferable access technology type based on network and inter-system mobility restrictions and provides information on access networks like WLAN hotspots that are available to the UE. It has to be noted that the usual 3GPP PLMN selection procedure to select the highest priority PLMN at a certain location is performed prior to any access network discovery and selection procedures based on ANDSF rules.

As mentioned, ANDSF can provide inter-system mobility policies, access network discovery information and inter-system routing policies to the UE. An inter-system mobility policy may e.g. indicate that inter-system handover from E-UTRAN to WLAN access is not allowed. It may also indicate that WiMAX access is more preferable than WLAN access when both are available. Inter-system mobility policies are a preference list of the accesses an UE should use at a given location and a given time. For access network discovery the ANDSF can provide information on access networks that are available in the UE's neighborhood including the access technology type like WLAN or WiMAX and access network identifiers like the WLAN SSID. Inter-system routing policies are applicable to UEs that are able to route IP traffic simultaneously over multiple radio interfaces (e.g. an IFOM capable UE). The operator can determine which type of traffic has to be routed through a certain radio interface. This include rules deciding when an access technology type or access network is restricted for a specific IP traffic flow or a specific APN and selecting the most preferable access technology, access network or APN to route IP

traffic that matches certain criteria (e.g. traffic to a specific APN, traffic belonging to a specific IP flow or specific application traffic).

ANDSF is based on a client/server architecture (see the figure below). The interface between the ANDSF client running on the UE and the ANDSF server is called S14. OMA Device Management is used on S14 to provide data to the UE via push (server initiated) or pull (UE initiated) mode. Push mode may not be possible in all scenarios (e.g. behind Firewalls). S14 requires an existing connection between UE and ANDSF server via 3GPP or non-3GPP access.

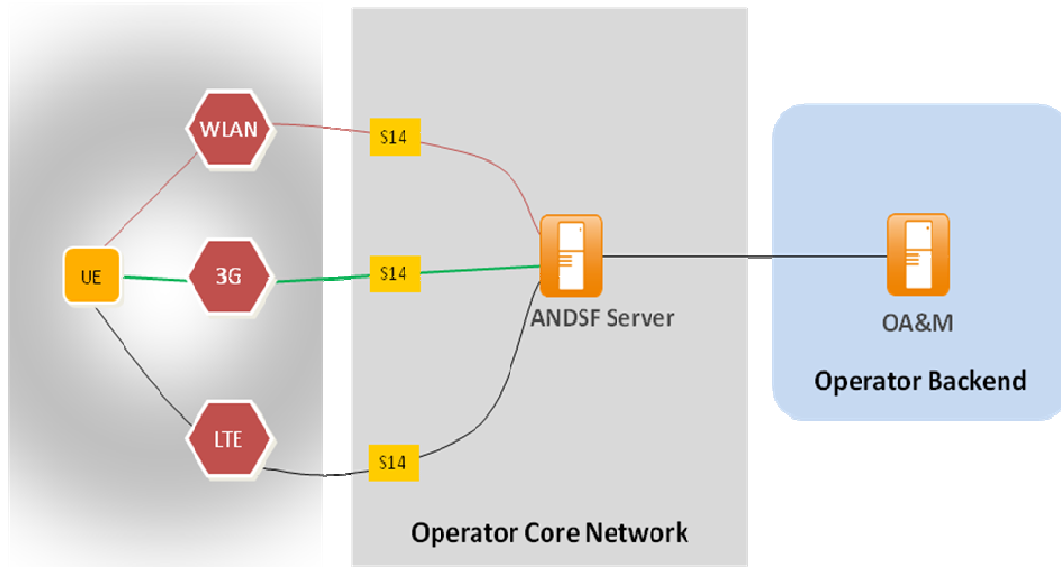


Figure A3-22: ANDSF architecture

The ANDSF server can be located in the home network (H-ANDSF) or in the visited network (V-ANDSF). In non-roaming scenarios the H-ANDSF is discovered through interaction with the DNS or DHCP server (ANDSF address or name can be provided in DHCP messages to the UE during IP address allocation). The H-ANDSF address or name may also be pre-configured in the UE. In roaming scenarios the V-ANDSF is discovered through DNS or DHCP.

More details on the ANDSF framework can be found in [3GPP_TS_23.402] and [3GPP_TS_24.302].

2.5.5 Relevance for MEVICO WP4

Understanding the currently standardized 3GPP functionality for IP offloading and access network selection is essential for discussing related enhancements in the scope of WP4.

3GPP has standardized several solutions to integrate WLAN access into 3GPP traffic.

- WLAN traffic can be offloaded to local IP access networks without seamless mobility to/from those networks
- To enable access to operator services, WLAN traffic can be routed through a PDN connection towards a 3GPP P-GW.
- For load distribution, a UE may simultaneously have PDN connections using WLAN and 3GPP radio access toward a 3GPP P-GW.

Access network selection for WLAN and WIMAX is performed by 3GPP UEs taking into account operator policies which are provisioned to the UE via the Access Network Discovery and Selection Function. Inter-system mobility policies are a preference list of the accesses an UE should use at a given location and a given time. For access network discovery the ANDSF can provide information on access networks that are available in the UE's neighborhood including the access technology type like WLAN or WiMAX and access network identifiers like the WLAN SSID. Inter-system routing policies are applicable to UEs that are able to route IP traffic simultaneously over multiple radio interfaces (e.g. an IFOM capable UE). The operator can determine which type of traffic has to be routed through a certain radio interface.

2.6 Service identification for improved radio utilization for GERAN (SIRIG)

2.6.1 Overview

Service identification for improved radio utilization for GERAN (SIRIG) enables GERAN to treat different applications differently.

Due to urgent demands primarily from Chinese operators, a limited solution (e.g. no PCC support, only GERAN Access) for the packet core and GERAN to enable was agreed in 3GPP (see [3GPP_TS_23.060], Clause 5.3.5.3). It is likely that this mechanism will be developed further in Rel-12.

2.6.2 Motivating use cases

A Popular Chinese Messaging Service leads to network congestion: Service can cope with limited bandwidth (1 GSM time slot), but GERAN resource management usually reserves more bandwidth (several time slots) once packet traffic is received. Machine Type Communication terminals also frequently use GERAN and require only limited bandwidth.

This leads to the requirement that traffic related to particular application (here messaging) needs to be detected and taken into account in radio resource management. For the applications above, a limitation of the resource reservation was envisioned, but it was also foreseen that an upgrading of QoS might be required for other applications.

As an additional complication for GERAN (which might also apply for UTRAN), many existing GERAN deployments only support a single PDP context / bearer per terminal, so 3GPP QoS differentiation mechanisms based on several PDP context with different QoS classes cannot be used to give traffic related to certain applications a priority handling compared to traffic related to other applications of the same user.

2.6.3 Solution Overview

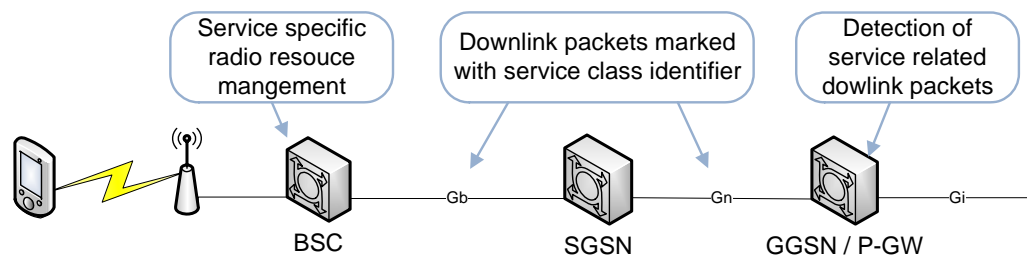


Figure A3-23: SIRIG solution

Downlink Traffic related to a particular application is detected in the core network GGSN (most likely using deep packet inspection). Related downlink user plane packets are marked with a Service Class Identifier. The GTP-U protocol (between the GGSN and SGSN) and the Gb interface protocol (between the SGSN and BSC) are extended to transport the Service Class Identifier. The BSC takes the service class into account for radio resource allocation.

No service class identifier values are standardized in Rel-11; the definition of services and the related improved radio utilization is left to operator policy.

2.6.4 Open Issues likely to be addressed in future work:

During the Rel-11 discussions, possible improvements likely be addressed in later Releases already surfaced:

Standardized Service Class Identifier Values would be necessary to reach a widespread roaming support of SIRIG and could also enhance the interoperability of equipment from different vendors..

The SIRIG concept and related GTP-U protocol extensions could also be applied for other RAN types. However, for other RAN types were real deployments support the current 3GPP QoS differentiation solution of multiple bearers with different QCI values per user, the missing definition of service class identifier values makes concerns about the unclear relationship and possible overlap of Service Class Identifier to current QoS concepts using QCI more urgent.

A control of SIRIG via Policy and Charging Control was already discussed extensively; see 3GPP Tdoc [C3-120798](#). Again, the relationship of Service Class Identifier to QoS related parameters (QCI, bandwidth parameters) as used in PCC complicated those discussions. Deep packet inspection can also be performed in a standalone TDF, but SCI marking to be performed in the GGSN based on those deep packet inspection results in the GGSN, where the GTP protocol is terminated, is problematic. For

charging traffic differently based on applied service class identifier, the lacking feedback from RAN if special treatment was indeed applied was found problematic.

2.6.5 Relevance for MEVICO WP4

Understanding the 3GPP SAE QoS concepts is essential for discussing possible enhancements within the scope of WP4.

Current 3GPP QoS mechanisms are not yet widely supported, in particular for GERAN access. 3GPP has defined a limited alternative mechanism for GERAN in Rel-11: Downlink Traffic related to a particular application is detected in the core network GGSN / P-GW (most likely using deep packet inspection). Related downlink user plane packets are marked with a Service Class Identifier (SCI). The radio network takes the service class into account for radio resource management (RRM).

This solution is likely to be extended in future 3GPP work, e.g. by enhancing the policy control support and by extending the solution to other radio access network types.

2.7 User Plane Congestion Management (UPCON)

2.7.1 Overview

Mobile operators are seeing significant increases in user data traffic. For some operators, user data traffic has more than doubled annually for several years. Although the data capacity of networks has increased significantly, the observed increase in user traffic continues to outpace the growth in capacity. This is resulting in increased network congestion and in degraded user service experience. Reasons for this growth in traffic are the rapidly increasing use of smart phones and tablet like devices.

3GPP is studying improvements to allow using the available resources during radio network is such a manner that an optimal mix of high priority services and applications, and users with premium subscriptions is supported, while maintaining the user experience, and supporting as many active users as possible.

2.7.2 Status in 3GPP

A Stage 1 Study on Use Cases and Requirements for User Plane Congestion Management (UPCON) in 3GPP [3GPP_TR_22.805] has been completed in September 2012. This TR considers scenarios and use cases where high usage levels lead to user plane traffic congestion in the RAN, and proposes potential requirements for handling user plane traffic when RAN congestion occurs. A work item to start normative stage 1 and stage 2 work has now been agreed ([S2-124145](#)); it includes the following work:

- Normative Stage 1 requirements based on TR conclusions have been added into TS 22.101 in 2H2012. The results of the TR are summarized below.
- Stage 2 work has started with a study on related solutions in new TR [3GPP_TR_23.8yz_UPCON], which is planned to be finalized in September 2013. As a first step, so called key-issues to be investigated are being defined.
- Depending on conclusions of this study, the WID will be updated to include affected normative specifications. Completion of the normative stage 2 and stage 3 in Rel-12 is envisioned, but it is too early to assess if this can really be accomplished.

2.7.3 Some Considered Use Cases

Use Cases considered in [3GPP_TR_22.805] include the following:

- User traffic of user with “platinum” subscription is served with priority during RAN congestion
- User traffic of “heavy” users (e.g. Users who exceed some monthly volume quota according to their subscription) obtains only a limited bandwidth during RAN congestion.
- When the RAN is congested, the data rate of some applications such as P2P applications or software updates is limited.
- A specific communication service is allocated resources preferentially while a cell is congested due to high data traffic volume during a disaster situation.
- Content Delivery “push” services are only executed when RAN is not congested
- Traffic compression, transcoding, application protocol optimizations (g. HTTP Multi-Part Response, HTTP Pipelining, ROHC), or triggering of Rate renegotiation for Voice or Video are executed only during RAN congestion (e.g. to limit negative impacts on user experience).
- UE informs network if traffic relates to user interaction (“attended traffic”) or background application activity (e.g. Software update), and radio resources for unattended traffic are reserved with lower priority or blocked during RAN congestion.

- The system informs users when RAN is congested and then charges data traffic with a higher rate.
- Most applications use the default bearer, but traffic related to some applications (e.g. software updates) is still treated with low priority or blocked during RAN congestion.

RAN Congestion can occur in single radio cells or the radio access network.

Many of the above use cases alternatively also apply not during observed RAN congestion but during known peak times, or for UEs at specific locations with known high traffic load.

2.7.4 Requirements

The following requirements have been identified in [3GPP_TR_22.805] and agreed as requirements for the ongoing stage 2 work:

General

- The network shall detect RAN congestion onset and abatement for a UE.
- The network operator shall be able to configure or provision and enforce policy rules to best deal with RAN user plane congestion.
- The system should react in a timely manner to manage a congestion situation. (A short-duration burst of user plane traffic should not be identified as RAN congestion.) Mechanisms to cope with RAN user plane congestions should be resilient to rapid changes in the level of congestion.
- The signalling overhead in the system shall be minimized.

Prioritizing traffic

- The network shall be able to differentiate and prioritize different applications (e.g. social networking, OTT video, blogging, internet games, FTP, software patches and updates, non real time services, etc.) in order to provide these applications with appropriate service quality.
- During RAN congestion the operator shall be able to select communications that obtain preferential treatment and sufficient resources.
- The network shall be able to select specific users (e.g. heavy users, roaming users, etc.) and adjust the QoS of their existing connections and new connections depending on the RAN congestion status and the subscriber's profile.

Reducing traffic

- Based on RAN congestion status and according to operator policy, the network shall be able to reduce the user plane traffic load (e.g. by compressing images or by adaptation for streaming applications).
- The system shall be able to separately adjust the communication media parameters of different media involved in communication (e.g. media for voice and media for video portions) so that they consume less bandwidth in case of RAN user plane congestion..
- According to operator policy, the network shall be able to select specific applications and control the data rate of the identified applications based on RAN user plane congestion status, at the same time taking into consideration user related information (e.g. a "platinum" subscription user should have good experience even if experiencing congestion) and content type (e.g. text vs. image).

Limiting traffic

- The network shall be able to limit traffic from operator-controlled and/or third-party services based on RAN user plane congestion status for a UE, e.g. to defer Push services based on the RAN congestion status and operator policy.
- The system shall be able to apply different handling (e.g. be able to prohibit or delay) all or a particular selection of IP bearer service requests depending on whether a service request is for Unattended Data Traffic or Attended Data Traffic (for immediate rendering on the screen).

2.7.5 Key issues investigated in Stage 2 Study

The following key issues have been identified so far in the stage 2 study in [3GPP_TR_23.8yz_UPCON]:

RAN User Plane congestion mitigation

The majority of mobile data traffic (e.g. Internet or over-the-top services traffic) is currently delivered over the default bearers. This key issue addresses aspects how the system can effectively mitigate RAN

user plane congestion in order to overcome the negative impact on the perceived service quality for such data traffic.

The congestion mitigation measures include traffic prioritization, traffic reduction and limitation of traffic, and shall be able to manage user plane traffic across a range of variables including the user's subscription, the type of application, and the type of content.

A key challenge for congestion mitigation is to support subscribers with different service requirements (e.g. premium, flat rate or roaming users) and application traffic with different traffic characteristics (e.g. long-lived and short-lived traffic flows) without increasing the system-wide signalling overhead significantly.

The following aspects should be considered by a solution addressing this key issue:

- The type of congestion mitigation measures, i.e. QoS/QoE control/adjustment through traffic prioritization, traffic reduction or traffic limitation based on the congestion status.
- The location of congestion mitigation measures (e.g. in UE, in RAN, in Core, in both, or in connected IP networks such as IMS or Packet-switched Streaming Service).
- The criteria to decide which flows will be subject of traffic mitigation measures (e.g. the user's subscription class, the type of application or the type of content).
- The information that are needed to effectively enforce the mitigation measure (e.g. the RAN congestion status, the impacted users, the type of traffic – e.g. attended vs. unattended) and how this information could be obtained.
- The way operators are able to control congestion mitigation through policies.

RAN User Plane congestion awareness

Some network elements outside the RAN may need to become aware of the congestion status.

The following aspects should be considered by solutions that propose some form of RAN congestion awareness:

- Where in the network is awareness of RAN user plane congestion required?
- What information on the congestion (e.g. severity of congestion, etc.) is required to enforce appropriate mitigation measures?
- Which level of granularity for congestion awareness is required?
- In case the congestion status needs to be reported from the RAN towards other system entities:
 - What is congestion and how is it detected?
 - How often and when does the congestion status need to be indicated?
 - What information needs to be indicated (e.g. severity of congestion or cell information), also taking into account the balance between signalling/processing overhead and benefits (e.g. preciseness)?
 - How is the congestion status be indicated, i.e. in the user plane or in the control plane) and over which interfaces?

2.7.6 Relevance for MEVICO WP4

The majority of mobile data traffic (e.g. Internet or over-the-top services traffic) is currently delivered over the default bearers and is not using existing 3GPP QoS mechanisms. 3GPP is currently investigating improvements to differentiate traffic of different users and/or applications and treat it differently (e.g. by prioritization, compression, limitation) based on RAN congestion status and operator policy.

Related requirements have already been agreed, but the study of solutions is at its beginning.

The ongoing 3GPP study thus touches some items which are also in scope of WP4.

2.8 Abbreviations

3GPP	Third generation partnership project
ADC	Application detection and control
AGCF	Access Gateway Control Function
AGW	Access GateWay
AF	Application function
ALG	Application Level Gateway
ANDSF	Access Network Discovery and Selection Function
APN	Access point name
ARP	Allocation and retention priority
BBERF	Bearer binding and event reporting function
BER	Bit error rate
CDMA	Code division multiple access
CN	Core network
CS	Circuit switched
CSCF	Call Session Control Function
DRA	Diameter routing agent
EATF	Emergency Access Transfer Function
E-CSCF	Emergency CSCF
EDGE	Enhanced data rates for GSM evolution
eHRPD	Evolved high rate packet data
EPC	Evolved packet core
ePDG	Evolved Packet Data Gateway
EPS	Evolved packet system
E-UTRAN	Evolved UMTS Radio Access Network
GBR	Guaranteed bit rate
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS support node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS tunnelling protocol
H-PCRF	A PCEF in the HPLMN
HPLMN	Home PLMN
HSS	Home subscriber server
HSPA	High Speed Packet Access
IBCF	Interconnection Border Control Function
ICE	Interactive Connectivity Establishment
I-CSCF	Interrogating CSCF
IETF	Internet engineering task force
IFOM	IP flow mobility and WLAN offload
IM	IP multimedia
IMS	IP multimedia subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet protocol
IP-CAN	IP connectivity access network
I-WLAN	Interworking WLAN
LDF	Load Detection Function
LTE	Long Term Evolution
MBR	Maximum bit rate
MGCF	Media Gateway Control Function
MGW	Media Gateway
MME	Mobility Management Entity
MRB	Media Resource Broker
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSC	Mobile-services Switching Centre
NAI	Network Access Identifier
NNI	Network to Network Interface
OCS	Online charging system
OFCS	Offline charging system
OMA	Open Mobile Alliance
P-CSCF	Proxy call server control function
PCC	Policy and charging control
PCEF	Policy and charging enforcement function
PCRF	Policy and charging rules function
P-CSCF	Proxy CSCF
PDN	Packet data network
P-GW	PDN gateway
PLMN	Public land mobile network
PMIP	Proxy mobile IP
PS	Packet switched
QCI	Quality class identifier
QoS	Quality of Service
SAE	System Architecture Evolution
SC	Service Continuity
S-CSCF	Serving CSCF
SDF	Service data flow

SDP	Session description protocol
SGSN	Serving GPRS support node
SGW	Serving gateway
SIRIG	Service identification for improved radio utilization for GERAN
SIP	Session initiation protocol
SMOG	S2b mobility based on GTP
SMS	Short message service
SOAP	Simple object access protocol
SPR	Subscription profile repository
SRVCC	Single Radio Voice Call Continuity
SSL	Subscriber spending limits
STUN	Session Traversal Utilities for NAT
TAS	Telephony Application Server
TCP	Transmission control protocol
TDF	Traffic detection function
TFT	Traffic Flow Template
TS	Technical Specification
TR	Technical Report
UDC	User data convergence
UE	User equipment
UMTS	Universal mobile telecommunications system
UPCON	User Plane Congestion Management
UTRAN	UMTS Terrestrial Radio Access Network
VoIP	Voice over IP
V-PCRF	A PCEF in the VPLMN
VPLMN	Visited PLMN
WCDMA	Wideband CDMA
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless local area network