



Security And Interoperability in Next Generation PPDR
Communication Infrastructures



Project Number: 313296

Deliverable 6.1

Connectivity, QoS provisioning and Seamless Mobility for Hetnets - Intermediate

Scope	Scheduled deliverable
Lead Beneficiary	FIGO
Dissemination level	Public
Document creation date	21/Oct/2014
Document release date	08/Jan/2015
Contractual Date of Delivery	30/Nov/2014
Version	1.2
Status	Final

Abstract: Deliverable 6.1 describes SALUS enhanced PMR based services on top of LTE and IEEE 802.11 ad hoc networks and interworking solutions between TETRA and TETRAPOL systems. It also includes mechanisms for seamless handovers in multi-interface broadband PPDR networks. *This deliverable includes a RESTREIT UE Annex which contains security sensitive information.

AUTHORS

Name	Organisation	Email
Frank Brouwer	FIGO	frank.brouwer@figonet.com
Hugo Marques	IT	hugo.marques@av.it.pt
Luis Pereira	IT	luis.pereira@av.it.pt
Georgios Charalampopoulos	UPAT	giwrgoscharalampopoulos@gmail.com
Theofilos Chrysikos	UPAT	txrysiko@ece.upatras.gr
Tasos Dagiuklas	UPAT	ntan@ece.upatras.gr
Panagiotis Galiotos	UPAT	pgaliot@gmail.com
Jérôme Brouet	ALU-I	jerome.brouet@alcatel-lucent.com
Bruno Sousa	ONE	bmsousa@onesource.pt
Geert Heijenck	UTWENTE	geert.heijenck@utwente.nl
Bernd Meijerink	UTWENTE	Bernd.meijerink@gmail.com
Olayinka Adigun	KU	O.Adigun@kingston.ac.uk
Alexandros Ladas	KU	A.Ladas@kingston.ac.uk

QUALITY ASSURANCE TEAM

Name	Organisation	Email
Frank Reinert	FhG	frank.reinert@iosb.fraunhofer.de
Manfred Blaha	PSCE	manfred.blaha@gmx.net
David Jelenc	UL	david.jelenc@fri.uni-lj.si
Jernej Kos	UL	jernej.kos@fri.uni-lj.si
Denis Trček	UL	denis.trcek@fri.uni-lj.si

EXECUTIVE SUMMARY

SALUS focusses on design, implementation and evaluation of a next generation communication network concept for Public Protection and Disaster Relief (PPDR) agencies, supported by network operators and industry. The project will provide security, privacy, seamless mobility, Quality of Service (QoS) and reliability support for mission-critical PMR voice and broadband data services. WP6 focusses on PMR Services on PPDR Broadband Networks. Deliverable D6.1 is an intermediate deliverable on the aspects connectivity, QoS and seamless mobility.

The end-users formulate their requirements as a mix of services the PPDR network needs to provide to the users. They require that the services are provided with at least a predefined quality. In addition the services need to be provided continuously, also when the end-users are mobile. As PPDR operations are mission critical, the requirements are valid even under the most extreme conditions, resilience is a prerequisite.

This document addresses the translation of end-user requirements into requirements and solutions for connectivity, Quality of Service (QoS) and seamless mobility. The foreseen system comprises a combination of technologies and networks, so it can be seen as a heterogeneous network (HetNet).

The end-user requirements mainly define services on an operational level. A main challenge is to create solutions for the new broadband PPDR services, as the quality for TETRA and TETRAPOL services is already in place. The 3GPP Service Architecture Evolution (SAE) provides a service definition that is a very useful starting point to translate the operational end-user requirements into technical requirements that can be implemented. The SAE defines a structure to provide required differentiation in quality for various services. This QoS Class Identifier (QCI) framework suffices PPDR solutions and creates a suitable basis to apply LTE systems in PPDR networks.

QoS and mobility have strong implications on the network architecture. The LTE QoS mechanisms are the basis for the overall broadband PPDR network. The Policy and Charging Rules Function (PCRF) is the core of this architecture guaranteeing the service quality according to the QCI. The LTE architecture contains Access Class Barring as an additional feature that enables differentiation between different user groups to further guarantee the quality for end-users. WLAN also provides QoS mechanisms. The 802.11e version of the standard focuses on QoS. The main parameters are jitter, latency and packet loss, which are similar to the LTE QoS parameters, but do differ. In ad-hoc networks QoS is a challenge in itself. The lack of a central controlling unit or central registry requires other mechanisms to arrange for the guaranteed quality. Various architectures may solve this where the common denominator is that each node contains the functions of routing, scheduling, and admission control. The definition and handling of QoS requires unification between LTE, WLAN and ad-hoc networks. LTE is the selected starting point for this unification. The LTE QoS framework provides a good basis, and the PPDR network will have LTE in its basis. This unification required that WLAN and ad-hoc network components at least include the PCRF functionality of the LTE network.

This document also addresses mobility between systems and technologies. SALUS assumes IP as the universal transport technology for all services. As a result, inter-system mobility translates into IP-layer mobility. The end-user requires seamless communications, also when switching between systems. Mobile IP does provide mobility, but does not provide seamlessness. Proxy Fast Mobile IP (PFMIP) is a technology that may require sufficient seamlessness. The PFMIP technology only provides the mechanism to have a seamless handover of the IP connection. However, it requires the IP address of the new router as a prerequisite. Media Independent Handover (MIH) is a technology that can provide these IP addresses. Seamless communications implies combining MIH, providing the information, and PFMIP to execute the handover.

Network management is an important component in any network. The network management is crucial for the effectuation of QoS in combination with other aspects like security. A network management system comprises of components for fault, configuration, accounting, performance and security management. Configuration and performance management have a strong relation to QoS, but also have other dimensions. Network management has standard or technology related components, but also includes vendor specific selections of tools and/or options. TETRA, LTE, WLAN and ad-hoc Network Management System (NMS) solutions are to be found in the Command and Control Centre (CCC). Ad-hoc networks also require distributed NMS components that need to be synchronized with the central NMS when possible, but can act stand-alone if needed. This also relates to LTE based stand-alone solutions like 3GPP Proximity Services (ProSe) solution.

Overall, QoS and mobility form the basis of PPDR networks to provide IP connectivity with the required quality at the required location, with the required resilience.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
TABLE OF CONTENTS	5
TABLE OF FIGURES	7
TABLE OF TABLES	8
1 Introduction	9
2 Requirements.....	10
2.1 User requirements using the 3GPP QoS framework.....	10
2.2 QoS related requirements	13
2.3 Mobility related requirements	13
2.4 Reliability requirements	14
2.5 Security requirements	14
2.5.1 Confidentiality	15
2.5.2 Integrity/confidentiality.....	15
2.5.3 Availability	15
2.5.4 Miscellaneous	16
3 Architecture	17
4 Quality of Service mechanisms	19
4.1 LTE/SAE specific Quality of Service mechanisms	19
4.1.1 Brief overview of the LTE reference architecture	19
4.1.2 Congestion management – Access control to air interface	21
4.1.3 E2E LTE QoS framework	23
4.1.4 QoS and roaming	29
4.2 IEEE 802.11 specific Quality of Service mechanisms.....	31
4.2.1 Quality of Service mechanisms in hot spot systems	31
4.2.2 Quality of Service mechanisms in ad-hoc networks.....	34
4.3 Conclusion on Quality of Service solutions towards unification for an integrated solution	41
5 Mobility mechanisms	42
5.1 IP-layer mobility.....	42
5.1.1 Mobility Architecture	42
5.1.2 Proxy mobile IPv6	43
5.1.3 Fast handovers for proxy mobile IPv6	44
5.1.4 Multicast.....	45
5.2 Media Independent Handovers	47
5.2.1 MIH architecture.....	48
5.2.2 MIH Protocol Frame	50
5.2.3 MIH Transport mechanisms	52
5.2.4 MIH security considerations	53

5.2.5	QoS in MIH	53
5.3	Seamless mobility between LTE and other networks.....	53
5.4	QoS and PMIP for 802.11	58
5.5	Multicasting in mobile networks.....	60
5.5.1	Multicast mobility problems and multicast mobility support.....	60
5.5.2	Multicast Source and Listener Mobility	61
5.5.3	Multicast Listener Mobility	61
5.5.4	Base solution for mobile multicast source support in PMIPv6 networks.....	61
5.5.5	Multicast Challenges and QoS	64
6	LTE resilience aspects	65
7	Network management	66
7.1	Introduction	66
7.2	Network Management System (NMS)	66
7.2.1	FCAPS Model	67
7.2.2	Network Management Architecture	69
7.3	LTE Network Management System.....	69
7.4	WLAN ad-hoc Network Management System.....	71
8	Conclusions.....	72
	Bibliography	73
	Acronyms	76

TABLE OF FIGURES

Figure 1 – SALUS System/Security Architecture (interim release).....	18
Figure 2 – simplified view of LTE reference architecture (Release 10)	19
Figure 3 – Access Class Barring principle	22
Figure 4 – High Priority Access - principle	23
Figure 5 – EPS Bearer and QoS	24
Figure 6 – E2E LTE QoS framework – functional architecture	29
Figure 7 – Home routed roaming model (simplified – charging not depicted-)	30
Figure 8 – LTE local breakout architecture (simplified – without charging).....	30
Figure 9 – HCF control framework.....	32
Figure 10 – Legacy 802.11 station and 802.11e station with four ACs within one station	33
Figure 11 – The INSIGNIA architecture (adapted from: [14])	36
Figure 12 – DAIDALOS Architecture for (a) mobile node and (b) gateway (obtained from: [16])	37
Figure 13 – SWAN architecture (Obtained from: [17])	38
Figure 14 – HQMM Architecture (obtained from: [18])	39
Figure 15 – SALUS architecture proposal.....	43
Figure 16 – Proxy Mobile IPv6 architecture	44
Figure 17 – PFMIIPv6 predictive handover.....	45
Figure 18 – Protocol overview	46
Figure 19 – Example of MIH signalling for PFMIIPv6 handover	47
Figure 20 – MIH architecture with LTE and WLAN networks.	49
Figure 21 – MIH Architecture in a MN with several physical interfaces.	49
Figure 22 – Types of MIHF relationship (based on [50]).	50
Figure 23 – MIH Protocol Frame [50].....	50
Figure 24 – MIH Protocol Header format.	51
Figure 25 – MIH message encapsulated in an Ethernet frame.	52
Figure 26 – MIH message encapsulated in an IPv6 packet, using TCP as the transport provider.	53
Figure 27 – Mobility modules integrated into the standardized LTE/EPC architecture	54
Figure 28 – Horizontal Handover Signalling Flow	56
Figure 29 – Vertical Handover Signalling Flow	57
Figure 30 – Mobile multicast source support in PMIPv6 networks	62
Figure 31 – Mobile multicast source support in PMIPv6 networks - Movement of Mobile Node Receiver (MN2)	62
Figure 32 – Group communication in Multicast-deployed PMIPv6 networks	64
Figure 33 – LTE resilient architecture (simplified)	65

TABLE OF TABLES

Table 1 – LTE QCI definition	10
Table 2 – Translation of service requirements for D2.2 to QCI parameters.....	11
Table 3 – Applicability of UE access classes in Home and Visited PLMN.....	23
Table 4 – Default QCI parameters (from [3]).....	26
Table 5 – Challenges in providing QoS in IEEE 802.11e	32
Table 6 – Mapping between User Priority and Access Category	33
Table 7 – The basic building block of a cross layer approach	36
Table 8 – Main concepts within standard IEEE 802.21 [50].	48
Table 9 – Description on MIH Protocol Header fields (based on [50] and [51]).	51
Table 10 – IEEE 802.11 and PMIPv6 QoS Connection mapping.....	58
Table 11 – WMM and PMIPv6 QoS Connection mapping	58
Table 12 – QoS Mapping between QCI/DSCP, 802.1D UP, WMM AC	59
Table 13 – Admission Controlled Flows - Bandwidth Parameters.....	59

1 INTRODUCTION

This document provides an intermediate description of how connectivity, Quality of Service and seamless mobility can be realized over heterogeneous networks. The document in particular focuses on providing communication over multi-interface broadband PPDR networks. Regarding connectivity, this document investigates interoperability solutions for IP data transfer and roaming over heterogeneous networks consisting of public LTE, private LTE, public IEEE 802.11 hotspot networks and private IEEE 802.11 ad-hoc networks. Mobility with TETRA and TETRAPOL networks are handled on application level and are described in deliverable 6.2.

The aim of the solutions is to provide automatic bearer selection mechanisms that provide continuous connectivity with data link persistence and meet the QoS, Quality of Experience (QoE) and resilience demands for PPDR applications. IP connectivity in particular targets new services such as streaming video, database access, file transfer, positioning and navigation, while supporting TETRA/TETRAPOL compatible push-to-talk services. The solutions are derived from the use cases defined in WP2 and the system architecture and requirements defined in WP3.

WP2 provided functional requirements in generic terms. Section 2 of this document provides the translation of these WP2 requirements into technical requirements. Section 3 provides a description of the SALUS system architecture related to Quality of Service and mobility mechanisms. Section 4 describes Quality of Service mechanisms for LTE, IEEE 802.11, ad-hoc networks and provides a first approach in uniting the mechanisms for an integral solution for PPDR. Section 5 describes mobility mechanisms in two additional mechanisms - IP-layer mobility and Media Independent Handover. Section 6 provides a description of resilience aspects for LTE. Sections 7 and 8 describe network management systems. The first section provides the general approach, while the latter section describes specific solutions for different system components.

2 REQUIREMENTS

This section describes the requirements for connectivity, quality of service and seamless mobility in heterogeneous networks when applied for use by Public Protection and Disaster Relief users. User requirements for the overall system can be found in SALUS deliverables 2.2 [1] and 2.4 [2]. This section translates the user requirements into technical requirements. The list of technical requirements is not exhaustive, but rather aims to contain those requirements that are important for the research into the principle aspects of the system.

2.1 User requirements using the 3GPP QoS framework

3GPP provides a QoS framework in [3]. This framework is very suitable for translating end-user service requirements into technical requirements of the services. Within this framework, services are classified in a total of 9 pre-defined classes. Each of these classes is identified with a QoS Class Identifier (QCI). The QCI defines the service type (yes/no GBR: Guaranteed Bit Rate), maximum packet delay and maximum error rate, as shown in Table 1. The selection of the QCI for an application and the priority can be defined by the operator. The priority values and applications are strongly recommended, but are not mandatory.

Table 1 – LTE QCI definition

QCI	Type	Prio	Packet Delay	Error Rate	Examples
1	GBR	2	100 ms	10^{-2}	Conversation voice
2		4	150 ms	10^{-3}	Conversation video
3		3	50 ms	10^{-3}	Real-time gaming
4		5	300 ms	10^{-6}	Streaming video
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}	
8		8	300 ms	10^{-6}	
9		9	300 ms	10^{-6}	

This framework needs to be filled in by the system designer/operator. The QCI does not define bandwidth. The priority and application can be selected and the admission/retention mechanisms need to be added. SALUS deliverable 2.2 [1] provided end-user requirements in terms of the required applications. Table 2 shows this table, where the end-user requirements in terms of applications are translated to QoS requirements according to the LTE/SAE QoS framework.

Table 2 – Translation of service requirements for D2.2 to QCI parameters

Category	Item		QCI	GBR	Prio	MBR	Delay budget	Packet loss	Remark
Group Voice	*Group call		1	√	2	12.2 kbps	100 ms	10 ⁻²	
	Late entry		5	✖	1	-	100 ms	10 ⁻⁶	Signalling for group call
	Dynamic reassignment		5	✖	1	-	100 ms	10 ⁻⁶	
	Prioritisation within group		5	✖	1	-	100 ms	10 ⁻⁶	
	Only 1 person to speak		5	✖	1	-	100 ms	10 ⁻⁶	
	Fast call set-up		5	✖	1	-	100 ms	10 ⁻⁶	
1-2-1 Voice	Point to point		1	√	2	12.2 kbps	100 ms	10 ⁻²	
	Telephony		1	√	2	12.2 kbps	100 ms	10 ⁻²	
Group video	*Group video streaming		2	√	3	500 kbps	150 ms	10 ⁻⁶	
	Late entry		5	✖	1	-	100 ms	10 ⁻⁶	Signalling for group video
	Dynamic reassignment		5	✖	1	-	100 ms	10 ⁻⁶	
	Prioritisation within group		5	✖	1	-	100 ms	10 ⁻⁶	
	*Video from ad-hoc fixed locations to CC		4	√	3	500 kbps	300 ms	10 ⁻⁶	Interpreted as surveillance
	*Video on location for local use (unit-commander)		2	√	3	500 kbps	150 ms	10 ⁻⁶	Requirement for ad-hoc network
1-2-1 Video	Video streaming		4	√	3	500 kbps	300 ms	10 ⁻⁶	
Emergency voice	Pre-emptive priority	Common for all	1	√	2	12.2 kbps	100 ms	10 ⁻²	User plane
	Open microphone		5	✖	1	-	100 ms	10 ⁻⁶	Control plane
Data Applications	Instant messaging		6	✖	6	-	300 ms	10 ⁻⁶	
	Email		8	✖	8	-	300 ms	10 ⁻⁶	
	Automatic number plate/license plate recognition		9	✖	9	-	300 ms	10 ⁻⁶	

Category	Item	CQI	GBR	Prio	MBR	Delay budget	Packet loss	Remark
	Picture messaging	8	×	8	-	300 ms	10^{-6}	
	Remote controlled CCTV	4	√	3	500 kbps	300 ms	10^{-6}	
	*Sending location data (vehicle/person) to CCC	6	×	6	-	300 ms	10^{-6}	
	*Broadcasting location from CCC to units	6	×	6	-	300 ms	10^{-6}	Requirement on MBMS
	Augmented reality	7	×	7	-	100 ms	10^{-3}	
	Augmented reality - text to voice	7	×	7	-	100 ms	10^{-3}	
	*Fingerprint scanning	9	×	9	-	300 ms	10^{-6}	
	DNA testing	9	×	9	-	300 ms	10^{-6}	
	*Patient monitoring (e.g. ECC)	6	×	6	-	300 ms	10^{-6}	
	*Monitor personnel's vital signs (drop detection, stress, toxicity levels...)	6	×	6	-	300 ms	10^{-6}	
	Location services	9	×	9	-	300 ms	10^{-6}	Is a collection of services with different QoS
Air to ground	Integration with aircraft communications	Relates to a collection of services. The QoS requirements for these services need to be supported by the air-to-ground link.						
Mobile ad hoc networks	Local broadband data communication facilities	Relates to a collection of services. The QoS requirements for these services need to be supported by mobile ad-hoc network.						
	Capacity extensions							
Database searching	*(Operational database search)	9	×	8	-	300 ms	10^{-6}	
	*Query cargo information (from crashed vehicles)	9	×	9	-	300 ms	10^{-6}	
	*Remote medical database services	9	×	8	-	300 ms	10^{-6}	
	*Car crash recovery system (cutting open crashed cars)	9	×	9	-	300 ms	10^{-6}	
Broadcast Voice	*Site related	Common for all	√	2	12.2 kbps	100 ms	10^{-2}	User plane
	Talk Group related							

Category	Item		QCI	GBR	Prio	MBR	Delay budget	Packet loss	Remark
	Geography related		5	✖	1	-	100 ms	10 ⁻⁶	Control plane
	Function related								
Broadcast Image	Site related	Common for all	2	√	3	500 kbps	150 ms	10 ⁻⁶	User plane
	Talk Group related								
	Geography related		5	✖	1	-	100 ms	10 ⁻⁶	Control plane
	Function related								
Interoperability			This implies that QoS shall be harmonized over technologies and deployment scenarios						
Local range extender	Incident comms	This implies that ad-hoc network and other range extender systems need to be transparent to QoS							
Crowd Control	Loudspeakers	1	√	4	12.2 kbps	100 ms	10 ⁻²		
	Geo-cast (via LTE) of alarms	8	✖	8	-	300 ms	10 ⁻⁶		Requires MBMS Interface to outside the PPDR network
	Evacuation procedures, etc via mobile phones,	8	✖	8	-	300 ms	10 ⁻⁶		
	Use of the screens at the stadium and outside	This reflects a larger group of applications that need to be detailed before QoS requirements can be formulated							

Table 2 shows that most service requirements can be filled in using the LTE QoS framework. There is however a number of functionalities that are not expressed as a service but rather as a system characteristic. These requirements need additional attention. In addition, the mapping to the LTE QoS needs to be carried into the overall system, also implying a number of additional requirements.

2.2 QoS related requirements

Some additional requirements related to QoS need to be fulfilled:

- The QCI definition of services shall be unified over all sub-systems of the network.
- Sub-systems shall have admission and retention capabilities in order to implement QoS.
- Sub-systems must obey the QCI information in their QoS mechanisms.
- QoS mechanisms shall retain the ability to perform basic operation when disconnected from the core network.

2.3 Mobility related requirements

The following requires relates in particular to mobility:

- End-user applications must retain connectivity in case of end-user mobility within networks.
- End-user applications must retain connectivity in case of end-user mobility between networks.

2.4 Reliability requirements

The SALUS infrastructure must provide a stable and resilient working platform for PPDR applications. These requirements should include a stable and easy to operate management system, offer resilient service delivery and a high level of availability (commonly achieved using redundancy and backup, fall-back and auto-recovery, self-organization). In the event of the network failure or loss of network coverage, direct communications without network infrastructure (in TETRA/TETRAPOL: Direct Mode Operation (DMO), in LTE: ProSe (Proximity Service)) between PPDR users is required as an immediate solution for re-establishing communications. Methods of achieving direct communication between users are also needed either through deliberate user action or as a result of devices leaving the network coverage.

The overall reliability requirement can be broken down into the following requirements [4]:

- The PPDR infrastructure must provide support of communication operations in any possible environment. The devices used (fixed and mobile) must be adaptable to a wide range of environments;
- The infrastructure needs to overcome failures related to extreme environmental conditions, natural as well as technical and man-made disasters. In failure situations, fast deployable solutions should provide communication services common to different PPDR forces, such as direct mode operation (DMO);
- The PPDR networks should be robust enough to support day-to-day operations, as well as emergency and other large events, being able to support solutions requiring high data rates, video and multimedia, used by PPDR agencies and organizations;
- The PPDR communications networks must support multi-link encrypted channels and the network must be able to prioritize traffic based on pre-defined parameters, to support QoS and pre-emptive emergency services.
- The PPDR networks should be capable of operating according to national Electro Magnetic Compatibility (EMC) regulations and must have some degree of quality concerning service delivery in the most critical communications. Adherence to national EMC regulations may be required between networks, radio communications standards and co-located radio equipment as defined in [5].
- The mobile device must be supporting power efficiency mechanisms and must be suitable for vehicle usage and/or to be operated as a hand held device;
- The system must be self-sustained. The organization must foresee the design of a network for high availability; for instance diversity, redundancy, automated failover protection, backup operational processes;
- Network and operational testing should take place to ensure that data and call processing functionality are restored within predetermined and guaranteed time period following a shutdown.

2.5 Security requirements

This section describes the security requirements in heterogeneous PPDR networks with broadband support, which are of the utmost importance to PPDR forces. In general, security requirements should include advanced encryption technology for air interfaces and end to end

encryption, enhanced authentication mechanisms for users, terminals and networks, efficient integrity protection, and support for third-party key management centre, for authorization management and over-the-air key updating. In addition to these system-level requirements, suitable operational procedures should be developed to accomplish required levels of security for information being passed across the network. Efficient and reliable PPDR communications within a PPDR organization and between various PPDR organizations, which are capable of secure operation, may be required. Key security requirements for PPDR systems with heterogeneous entities can be found in the following paragraphs [7]:

2.5.1 Confidentiality

- The access the PPDR organization should be authorized only to appropriate users. This should be implemented on network equipment, as well as on device (fixed and mobile) and on application level.
- Each network device and user should acquire a unique identifier and the association has to be strong enough for no further user interaction during the process. For instance, if the devices support the option for multiple users, each one should have its own authentication.
- The authentication service should use open standard protocols [8] and for ideal scenarios, to maximize security requires, mutual authentication from participating parties should be implemented. This way, the system is protected simultaneously from fake intruder base stations and devices.
- An administrative interface should be used as a management platform for authorization control. If the PPDR organization supports the option for user authentication, the administrative interface should provide options for user account management, such as adding, editing and suspending or deleting.
- The network should be equipped with mechanisms keeping track and recording all device or user access attempts and all authentication and/ or authorization procedures, including changes to authentication and authorization data stores as audit trails or other forms of evidence.
- The administrative interface of a PPDR organization should be able to terminate active sessions of individuals or user groups.

2.5.2 Integrity/confidentiality

- End-to-end encrypted communications are needed for mobile-to-mobile, dispatch and/or group calls communications [5]. Only authorized entities should have access to the exchanged information, so cryptographic controls must be applicable over all wireless links. Both point-to-point and point-to-multipoint traffic should be supported.
- In order to achieve continuous service provision, without the need for re-authentication for new distributions of cryptographic keys, the network must support periodic re-keying.
- Cryptographic controls are also needed to ensure that no modification has occurred to the transmitted information.

2.5.3 Availability

- Power backup for the elements of the network's infrastructure shall contain backup battery, UPS and/or power generation.
- Individual network elements should be highly reliable (99.999%). Ensuring adequate supply and easy access to spare parts will reduce Mean Time To Repair (MTTR). Operational readiness should be assured even in a maintenance window.

- Redundant elements must detect failure at the spot and automatically activate themselves to provide service upon failures of primary network components. (also called hot stand-by)

2.5.4 Miscellaneous

Some requirements do not correspond directly to any of the previously mentioned categories, but they improve the overall provided security:

- Need for third party key management system.
- Need for Over-The-Air (OTA) key update.
- Connections to the network shall have time-outs in order to avoid or repair deadlock situations. Such timeout shall have different limits depending on the transmission status of devices.
- Each PPDR organization should be capable of configuring its own timeout limits.
- The PPDR network must be capable of intrusion detection and attack monitoring.

3 ARCHITECTURE

The future PPDR communications system will be a system of systems, combining various interfaces. Legacy systems like TETRA and TETRAPOL will be combined with:

- current and future cellular systems complying to the 3GPP standards family;
- IEEE 802.11 based systems configured either as WLAN hotspot system or as ad-hoc network;
- Body Area Networks;
- Other systems like satellite systems (yet not on the scope of SALUS);

Figure 1 previews the components for the SALUS System/Security Architecture (additional details can be obtained in SALUS deliverable 5.2 [6] and in the upcoming deliverable 3.2 (Enterprise and System Architecture – Intermediate). The common denominator for all the depicted systems is the use of IP as transport mechanism. IP can be seen as a middleware layer, decoupling the application from the radio access methodology. Providing IP connectivity between the application endpoints with the QoS as required suffices. The connection to TETRA and TETRAPOL are also IP based, even though these systems are non-IP services.

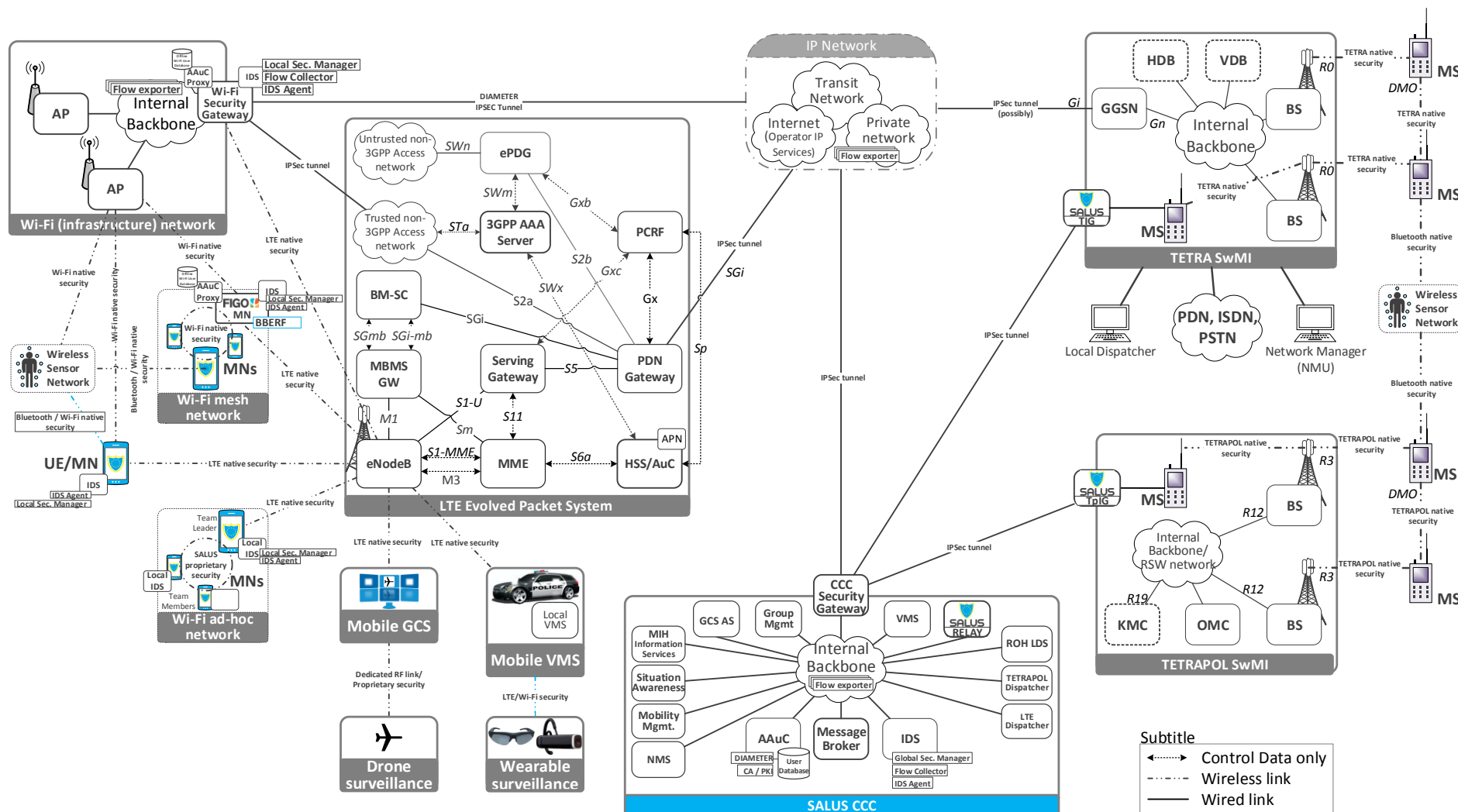


Figure 1 – SALUS System/Security Architecture (interim release)

4 QUALITY OF SERVICE MECHANISMS

4.1 LTE/SAE specific Quality of Service mechanisms

LTE is an all-IP cellular system offering broadband multimedia capabilities. Unlike the previous generation of cellular systems, all services (voice, data and video) are sharing the same packet based system. To ensure differentiated and guaranteed transmission of services with different characteristics (e.g. data rate, latency, jitter and packet error rate), LTE provides, since its first release, a comprehensive and sophisticated end-to-end QoS toolbox.

This end-to-end QoS toolbox is a key asset for PPDR organizations that will use LTE as an access technology in the future. However, this toolbox may not be the only tool that LTE brings to help PPDR organizations getting priority and guaranteed access over LTE. Indeed, according to different deployment scenarios (dedicated network and/or use of commercial networks), it may be desirable to make use of other tools when the network is congested. These tools include:

- Access control to air interface – for preventing non-authorized user to get access to the LTE network (Access Class Barring) or providing high priority access (can be used when getting services from a commercial operator)
- Control of use resources – an End-to-End (E2E) QoS framework enabling differentiated and guaranteed service delivery (applicable to dedicated PPDR LTE network or when using commercial networks),
- Roaming options and QoS (applicable to dedicated PPDR LTE network or when using commercial networks)

The following sections are providing details on these topics. Before entering into the details of QoS over LTE, a brief overview of the LTE architecture is given since most of the LTE functions have a role to play in the QoS.

4.1.1 Brief overview of the LTE reference architecture

Figure 2 (based on [4]) gives a simplified view of the reference architecture of an LTE network (release 10).

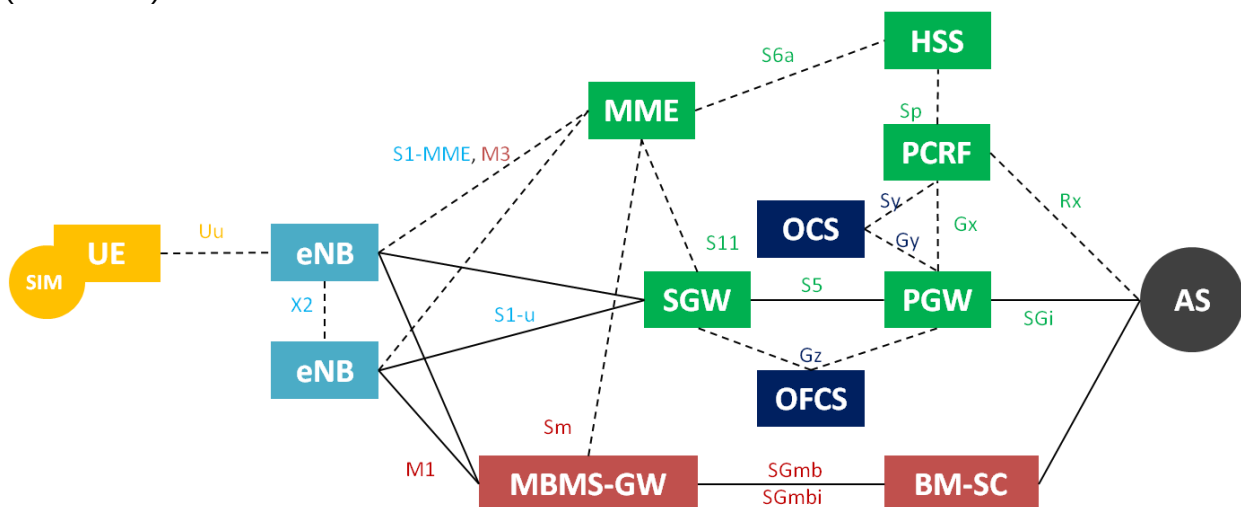


Figure 2 – simplified view of LTE reference architecture (Release 10)

The different elements of the reference architecture are the following:

- UE (User Equipment)
 - UE – it terminates LTE radio interface and provides IP transport for end-user traffic,
 - SIM (Subscriber Information Module) – it provides authentication of securely stored subscriber information and negotiates encryption keys and session protection
- E-UTRAN (Enhanced UMTS Terrestrial Radio Access Network)
 - eNB (eNodeB) – it provides LTE radio access including radio layer encryption, terminates network interfaces and maps radio access bearers to LTE radio bearer (QoS – radio access control and scheduling). Also responsible for Mobility Management Entity (MME) selection and forwarding of Non Access Stratum (NAS) signalling. Also responsible for mobility control between eNB and includes the MBMS Control Element function (MCE, not depicted in the chart) (MBMS = Mobile Broadcast and Multicast Service)
- Evolved Packet Core (EPC)
 - PGW (PDN Gateway) – it acts as end-user IP layer first hop router and IP anchor point for a given Packet Data Network (PDN). The PGW is responsible for mapping IP flows into Evolved Packet Core (EPS) bearer (QoS), assigning IP address to end-user. It provides charging information, QoS with Policy Enforcement and legal interception.
 - SGW (Serving Gateway) – it provides traffic routing through GTP tunnels between one or more PGW (S5) and eNB (S1-u), detects incoming end-user traffic for idle UEs and notifies MME.
 - MME (Mobility Management Entity) – it manages UE authentication, LTE RAN connection (S1-MME) and mobility and bearer establishment. It selects SGW and PGW and manages MBMS service and legal intercept on control signalling.
 - PCRF (Policy Charging and Rating Function) – it provides QoS and charging policies to the PGW (possibly transformed by PGW into operations on EPS bearers); the policies are obtained from different sources including SPR (HSS) and service requirement from the Application Server (AS)
 - HSS (Home Subscriber Server) – central database for subscriber data and user service profile performing user and network access authentication and mobility management function.
- Multimedia Broadcast and Multicast (will be leveraged from 3GPP release 12 to enable efficient support of PPDR group communications based on GCSE – Group Communications System Enablers)
 - BM-SC (Broadcast and Multicast Service Control) – it acts as a gateway between application server providing broadcast content and MBMS gateway (SGmb for control and SGmbi for traffic). It also provides UE MBMS error reception handling.
 - MBMS-GW (Multimedia Broadcast and Multicast Service Gateway) – it provides IP source of multicast flow to eNB (M1) and forwards service requests from BM-SC to MME (Sm).
- Charging
 - OCS (Online Charging System) – it performs online credit control function for pre-paid and data capped post-paid subscribers
 - OFCS (Offline Charging System) – it collects charging records for post-paid subscribers.

4.1.2 Congestion management – Access control to air interface

The mechanisms described in this section are of primary interest when a PPDR organization gets broadband services from a commercial operator. In that situation, the PPDR users and the commercial users are sharing the same access network and the E2E QoS framework may provide some guarantee of services (see 4.1.3). It may be required for the commercial operators to implement both of the following features to help ensuring PPDR users to access to the commercial service even in congested situations.

4.1.2.1 Access Class Barring

Access Class Barring is a feature that can be implemented by a mobile operator to limit or prevent pre-defined categories of UEs from making access request to the network in some congested situations.

The access class barring mechanism is defined in [10]. It relies on a set of parameters:

- UE access classes:
 - 0-9 for regular UEs
 - 10: for emergency calls (e.g. 112)
 - 11: for Public Land Mobile Network (PLMN) use
 - 12: for security services (e.g. PPDR)
 - 13: for Public Utilities
 - 14: for Emergency Services (e.g. PDDR)
 - 15: for PLMN staff
- Barring rate (a percentage that defines the probability of regular UEs to make an access request for outgoing calls); this value is a parameter that is set by the operators and can be updated and applied on a set of cells
- Flag per access special access class (10 to 15) to indicate which access class can access to the network.

These parameters are transmitted on the signalling broadcast channel in the System Information Base (SIB) Type2 messages.

It is to be noted that the Access Class Barring mechanism:

- Applies to both data and signalling access requests attempts,
- Only applies to outgoing calls; if a terminal receives an incoming call from an external network, it will answer to the request to get a connection, whatever the barring rate is.

Figure 3 describes the principle of Access Class Barring.

In the nominal situation, before making an access request, a regular UE makes a random draw (between 0 and 1) and compare the result with the current barring rate parameter being broadcasted in the cell on the SIB Type message. If the random value is lower than the current barring rate, the regular UE actually proceeds to the access request over the air. It is to be noted in this case that special access classes can make access at any time independently from the barring rate value. As a consequence, this mechanism may provide a way to provide higher priority access to air interface for outgoing calls for PPDR users in nominal situation (if the barring rate is set to a low value for instance). Indeed, this needs to be agreed with the mobile network operator that may not want to disfavour its commercial subscribers.

In case of a major event, the PPDR organization may ask the mobile operator to set the access barring rate to 0% in a specific area (e.g. in a set of cells surrounding the event). This can be

done by Operation and Maintenance (O&M) setting of the operator. Once provisioned, the new barring rate will be broadcasted over the air in a few seconds. When the barring rate is set to 0%, no regular user can make any attempt to access the network for outgoing calls (traffic and signalling) and only authorized special classes can attempt to access to the network. This mechanism may avoid having congested cells in area where a major event occurs and gives some guarantee to PDDR users (if authorized) to get access to the network resource. It is to be noted however, that this requires having an agreement with the mobile network operator providing the service and that totally blocking outgoing calls from may not be the best solution since it may forbid to receive interesting information of an event (e.g. a scene shoot by a citizen's smartphone camera) or would generate high traffic from family members for incoming calls that would like to get connected to their relatives / friends that are in an emergency area. This mechanism, as indicated before, only applies to outgoing calls and does not prevent congestion coming from incoming calls.

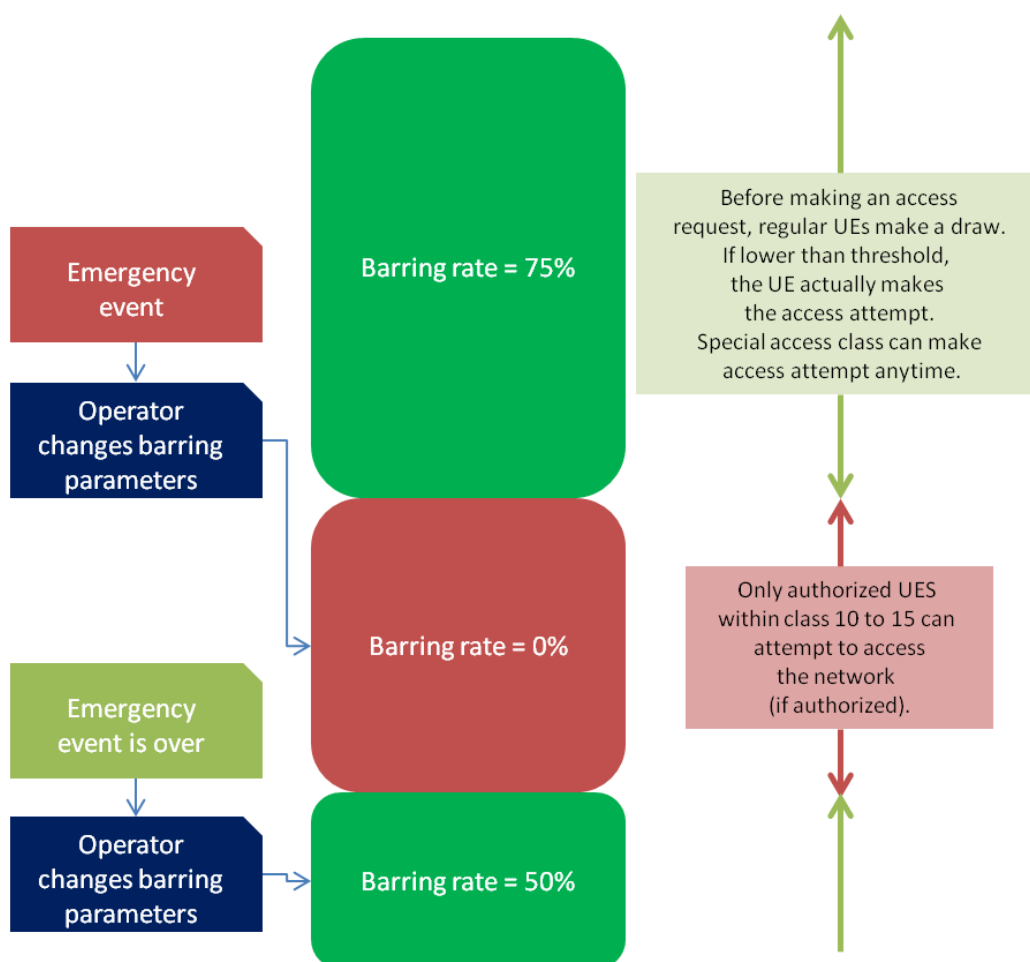


Figure 3 – Access Class Barring principle

Finally, it is to be noted that especially for the PPDR user access classes, this mechanism is only valid in PLMN network of the home country (see Table 3). The special PPDR access classes are applicable to both Home and Visited PLMN in their country. But, in case of cross border operations, if a PPDR user moves to a PLMN from a neighbouring country, he will then be considered as a regular UE.

Table 3 – Applicability of UE access classes in Home and Visited PLMN

Access Class	User	PLMN
0-9	Regular UE	Home and Visited PLMN
10	Emergency calls	Home PLMN and Visited PLMN, also without IMSI
11	PLMN use	Home PLMN
12	Security Services	Home and Visited PLMN but of home country only
13	Public utilities	
14	Emergency services	
15	PLMN staff	Home PLMN

In the 3GPP release 11, the service accessibility is being enhanced with additional mechanism (called Extended Access Class Barring – EAB). This primarily addresses machine type communications with delay tolerant applications. With this mechanisms, EAB enabled regular users are receiving additional information from the network (SIB Type 14 message) which indicates whether they are authorized or not to make access attempt irrespective of the barring rate value.

4.1.2.2 High Priority Access

High Priority Access is a feature that can be used by PPDR organizations when getting services from a commercial operator.

Figure 4 depicts the principle of this mechanism. When a UE from a special access class requests a connection, it indicates in the establishment clause “High Priority Access”. While in theory this may give higher priority to such UE, this approach also depends on the Call Access Control mechanisms and strategies that are provided by the manufacturer. Additionally, the operator has to activate this feature explicitly.

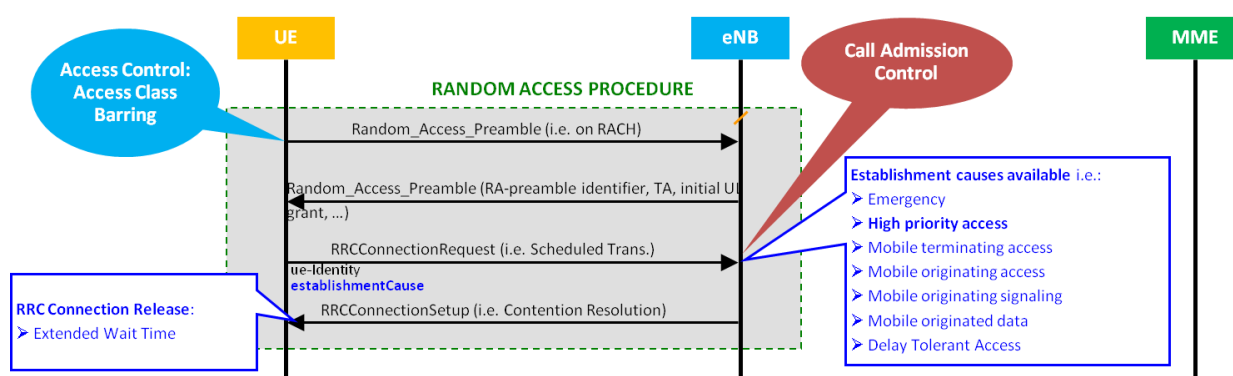


Figure 4 – High Priority Access - principle

4.1.3 E2E LTE QoS framework

The E2E LTE QoS framework consists of a standardized set of functions and mechanisms that ensure and enforce QoS along the journey of each packet in the LTE network from the PGW to the UE and vice versa (see [3]). This framework applies during all the phases of a PPDR user's session:

- At call admission - the system checks if there are sufficient resources to provide the required quality for the call; if yes, the call is granted with associated QoS parameters, if not, the system will look if it can pre-empt resources from lower priority sessions.
- During call – the system ensures that the QoS parameters of the service are maintained during the session according the pre-defined QoS parameters.
- During handover – the system ensures that the call quality will be maintained in the target cell in case there is a need to handover a session to a new cell.

The following section describes tools and architecture that enable such kind of capabilities. Indeed, these capabilities apply to all deployment scenarios. In the dedicated scenario, the PPDR organizations will have full control over the process explained hereafter whereas when getting services from a commercial MNO, the PPDR agencies will rely on the parameter settings and strategy of the MNO to implement QoS.

4.1.3.1 Principle of EPS Bearer

One of the main principles of the E2E LTE QoS relies on the concept of Evolved Packet System (EPS) Bearer, see Figure 5.

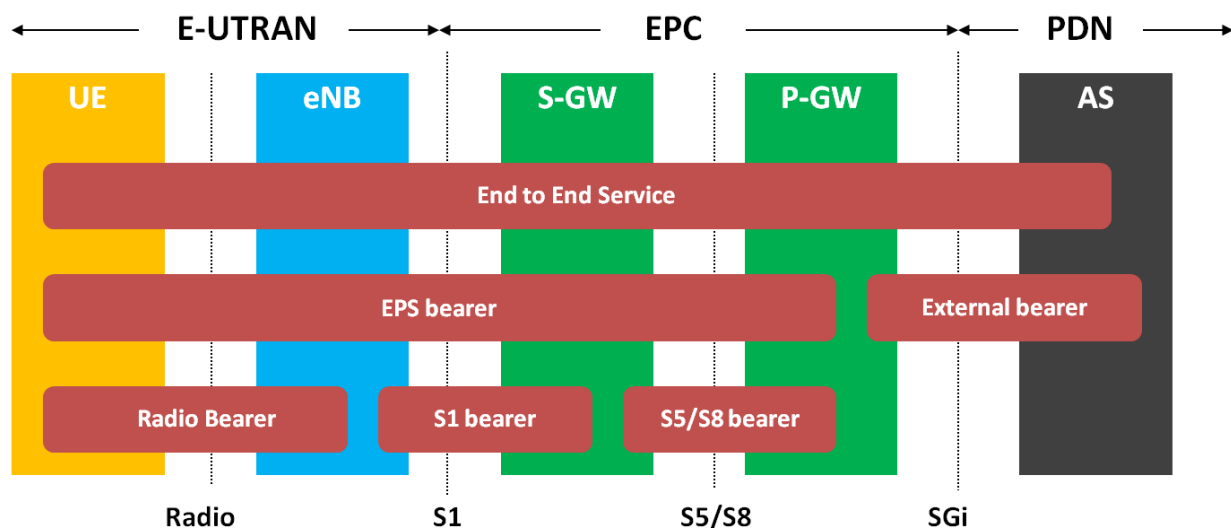


Figure 5 – EPS Bearer and QoS

An EPS bearer uniquely identifies packet flows that receive a common QoS treatment between the UE and the PGW (e.g. same scheduling/queue management/rate shaping policy). Every UE may have multiple EPS Bearers with different set of parameters enabling the transmission of multiple traffic flows in parallel with different QoS objectives. At the boundaries of the LTE systems (UE for uplink flows and PGW for downlink flows), each packet is examined and mapped to its associated EPS Bearer.

There are two types of EPS bearers:

- Default bearer,
- Dedicated bearer.

The default bearer is established during the attachment phase and maintained throughout the lifetime of the connection ensuring an always-on IP connectivity to the end-user. It is to be noted that multiple default bearers with different characteristics can be established at attachment

provided that each default EPS bearer has a different Access Point Name (APN). The EPS default bearer characteristics are provisioned in the HSS in the UE profile.

The dedicated bearers are usually established dynamically upon receipt of a service request initiated by either the terminal or the network. The method usually allows a better usage of the resource (dedicated EPS bearer are allocated only when needed). To enable dynamic EPS Bearer allocation, an interaction with the application server is necessary. For unicast traffic, this interaction is realized of the Rx interface (between the PCRF and the AS). In that case, the PCRF is a key component of the process.

Then, there are 2 categories of EPS bearers:

- Guaranteed Bit Rate – GBR,
- Non-Guaranteed Bit Rate – NGBR.

A GBR bearer is assigned a GBR at the bearer establishment. A non-GBR bearer is not associated with any GBR. The usage of a GBR bearer is justified when the service(s) carried over a GBR bearer shall not experience congestion-related packet loss and when precedence is given to service blocking over service dropping in congestion situations. The typical service that requires a GBR bearer is voice.

On the contrary, a NGBR bearer may experience congestion-related packet loss (e.g. the data rate of an ftp flow may be temporarily reduced or video packets of NGBR video flows may be delayed or dropped). In case of congestion, precedence is given to service dropping over service blocking.

It is to be noted that each EPS Bearer for each UE translates into lower level of bearers (Radio bearer, S1, bearer, S5 bearer) that maps the E2E QoS objective into sub-objectives for each interface crossed by each packet (radio, S1-u, S5). For simplicity, these will not be further discussed in this document.

4.1.3.2 LTE QoS parameters

Each EPS Bearer is characterized by a set of parameters that are used by the system to ensure guaranteed and differentiated E2E QoS. These parameters are:

- QCI – Quality of Service Class Indicator,
- ARP – Allocation and Retention Priority
- GBR (Guaranteed Bit rate) or AMBR (Aggregated Maximum Bit rate) for NGBR users.

Since the first release of LTE (3GPP Release 8), the 3GPP standard introduced the QoS Class Identifier (QCI) to ensure a minimum standard level of QoS to ease the interworking between the LTE networks mainly in roaming cases and in multi-vendor environments. Each bearer is assigned one QCI at bearer establishment. The QCI is further used within the LTE access network to define the control packet-forwarding treatment from an end-to-end perspective. As shown in and Table 4 (equal to Table 1), the following parameters characterize a given QCI:

- Resource Type: defines whether the bearer is GBR or non-GBR,
- Priority: defines a level of differentiation between SDF aggregates of the same UE or of different UEs (note, the lower the priority value is the higher is the priority),
- Packet Delay Budget (PDB): defines an upper bound delay that a packet is allowed to experience between the UE and the PCEF,

- Packet Error Loss Rate (PLR): defines an upper bound for the rate of IP packets that have been processed by the sender, but not successfully delivered by the receiver. Packet losses due to network congestion are excluded.

Table 4 – Default QCI parameters (from [3])

QCI	Type	Prio	Packet Delay	Error Rate	Examples
1	GBR	2	100 ms	10^{-2}	Voice
2		4	150 ms	10^{-3}	Live video (conversational or streaming)
3		3	50 ms	10^{-3}	Gaming
4		5	300 ms	10^{-6}	Buffered streaming video
5	Non-GBR	1	100 ms	10^{-6}	IMS signalling (default bearer for IMS APN)
6		6	300 ms	10^{-6}	High priority buffered streaming (video), TCP, etc
7		7	100 ms	10^{-3}	Medium priority voice, video, gaming
8		8	300 ms	10^{-6}	High priority best effort Internet
9		9	300 ms	10^{-6}	Best effort

The purpose of these parameters is to properly configure the scheduling in the eNB, SGW and PGW (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

It is to be noted that in principle, the parameters can be changed but to ensure consistency across all networks they should remain similar for a give QCI. The only parameter that can be transparently (and dynamically) modified is the priority associated to a QCI. This can be used in future PPDR networks to override priority on the LTE network.

It is also to be noted that for MBMS service only GBR QCIs apply ([11]).

In addition to the QCI, each bearer is assigned an Allocation and Retention Priority (ARP). The ARP contains 3 parameters that are further used in the admission control procedures:

- The priority level: defines the relative importance of the bearer request.
- The pre-emption capability: defines whether the incoming bearer request can pre-empt resources that are already assigned to an established bearer with a lower priority level.
- The pre-emption vulnerability: defines whether the bearer resources (once allocated) can be pre-empted to serve another incoming bearer request with a higher priority level.

The Aggregate MBR (AMBR) defines an upper limit of the aggregate bit rate consumed by a single subscriber across all the non-GBR bearers. Two different AMBR parameters can be distinguished:

- APN-AMBR: defined per UE and per Access Point Name (APN)
- UE-AMBR: defined per UE

Both parameters are separately defined for UL and DL and are provisioned in the LTE HSS. AMBR is an important parameter that allows network operators offering differentiated subscriptions in terms of maximum throughputs in UL and DL.

4.1.3.3 Temporary Flow Template

As explained before, packets are bound to the appropriate EPS bearers to ensure they can be treated appropriately by the LTE system. Packet filters are defined in the UE and the PGW to route respectively the UL or DL incoming packets over the appropriate EPS bearers. The Traffic Flow Template (TFT) is used to set the packet filters. A TFT is actually one packet filter or a set of packet filters associated with an EPS bearer. One can distinguish two types of TFT depending on the traffic direction: UL TFT and DL TFT.

The TFT contain a list of packet filters and each packet filter contains the following information:

- the identifier of the packet filter,
- the precedence of the packet filter,
- the direction (UL and DL),
- the filter itself.

The filter can be a pattern matching the IP 5-tuple (source/destination IP address, source/destination port number, protocol ID of the protocol above IP). In the pattern, an IP address may be combined with a prefix mask, a range of port numbers, or extended with IPv4 Type of Service or IPv6 Traffic Class and Mask. As an alternative, the filter may use other pattern detecting the IPSec Security Parameter Index or the IPv6 Flow Label.

Upon reception of a DL/UL incoming IP packet, the PGW/UE evaluates for a match, first the DL/UL packet filter that has the highest precedence and, in case no match is found, proceeds with the evaluation of DL/UL packet filters in decreasing order of their precedence. This procedure shall be executed until a match is found, in which case the DL/UL IP packet is transmitted on the EPS bearer that is associated with the TFT of the matching DL/UL packet filter. If no match is found, the DL/UL IP packet shall be sent via the EPS bearer that does not have any DL/UL packet filter assigned. If all EPS bearers (including the default EPS bearer for that PDN) have been assigned a DL/UL packet filter, the PGW/UE shall discard the DL/UL IP packet. The PGW provides the UE with the TFT description at bearer creation or bearer modification. The UE may request the modification of the packet filters.

4.1.3.4 Functional architecture

To have an efficient E2E QoS assurance and management over LTE, the QoS functions shall be implemented in a consistent manner throughout the LTE network. Figure 6 figure shows how the different QoS functions are distributed over the LTE network. It is to be noted that the functions have been grouped per level to highlight the links between them and ease the understanding.

At the application level, the UE interacts with the application servers. Upon an application request, the Application Function (AF) triggers the PCRF (through Rx interface) to apply a policy and charging treatment to appropriately serve the request.

At policy control level, the Policy and Charging Rules Function (PCRF) combines the session information received from AF, from the PGW and from the Subscription Profile Repository (SPR) that stores the subscriber data such as subscription rights and category. Then, the PCRF

decides whether to apply the resulting policy to the Policy and Charging Enforcement (PCEF) function in the PGW (through the Gx interface).

At the packet flow level, the PCEF enforces the policy control as indicated by the PCRF. The PCEF executes gate enforcement and QoS enforcement. Gate enforcement is the capability to block IP packets belonging to a given Service Data Flow (SDF) depending on the PCRF decision. The QoS enforcement allows the PCRF to provide the authorized QoS for a given packet flow. QoS enforcement encompasses:

- Per-user based packet filtering by using for instance Deep Packet Inspection (DPI),
- Rate policing per SDF, based on APN-AMBR in DL.

At the bearer level, the UE and the PGW implement packet filtering functions that map the SDF to the appropriated EPS bearer. Rate policing are executed per bearer in the UE, eNB and PGW based on AMBR, MBR and GBR parameters. Rate policing in UL may be activated in the SGW, especially in roaming configuration without local breakout. The key QoS functions per bearer are implemented in the eNB (it is to be noted that all of the functions above are supplier dependent):

- Radio admission: The eNB implements admission control to ensure the performance requirements on the GBR, the packet loss and latency. Pre-emption of on-going bearer(s) may be triggered depending of the ARP field setting.
- Radio bearer control: This function manages the establishment, modification or release of the bearers. At bearer establishment, the eNB shall set the L1/L2 radio parameters based on the QCI. This includes configuring parameters for HARQ or ARQ activation and retransmissions, and for the adaptation of the modulation and coding schemes as function of the radio conditions.
- Radio scheduler: the eNB schedules and allocates the UL and DL radio blocks to the UE in an efficient and optimized manner based on the QCI requirements and to ensure fairness between the end-users.
- Radio congestion control: The eNB is in charge of triggering mechanisms to address overload conditions that may occur on the radio or S1 interface.

The SGW is involved in the QoS management since it triggers the re-establishment of the S1 bearer upon receipt of a DL packet when the UE is in idle mode. Also, it shall correctly switch the S1 and S5 bearers per QCI and per user. Finally, the MME ensures the retrieval of the QoS parameters from the HSS and the establishment/release of the S1 bearers.

The transport level is also an important point of the end-to-end QoS to ensure a forwarding treatment on the terrestrial networks (backbone and backhaul) consistent with the QCI of the bearer. The eNB in uplink and the PGW in downlink mark the DSCP and p-bit of the outgoing packets as the function of the QCI. The SGW also performs packet marking in UL and DL. The marking allows traffic policing in the transport network and a QoS-aware forwarding in the intermediate transport nodes of the mobile backhaul network. In addition, functions such as traffic shaping, traffic congestion and admission management are required at transport level to guarantee end-to-end performances on the packet loss rate and the latency, especially when the mobile backhauling is provisioned with a high aggregation ratio.

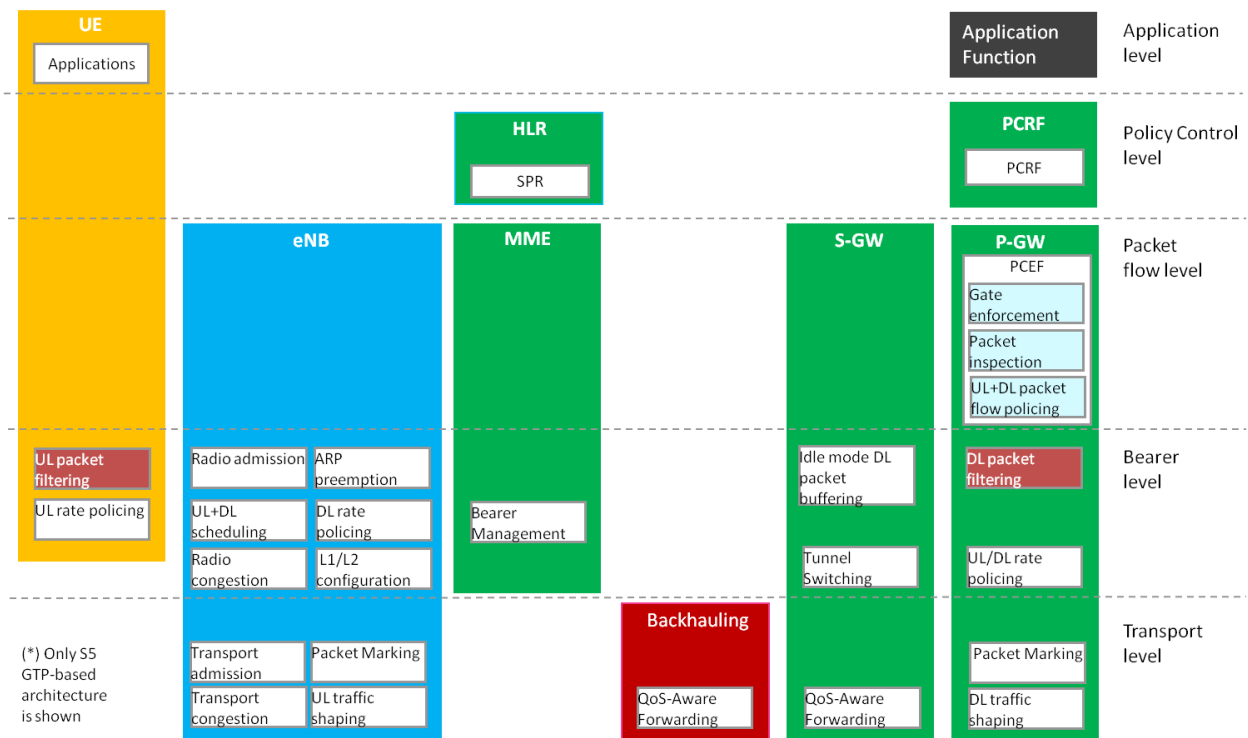


Figure 6 – E2E LTE QoS framework – functional architecture

4.1.4 QoS and roaming

In future mode of operations, PPDR users using LTE may need to roam into another network:

- A visited PLMN from another PPDR organization in a foreign country,
- A visited PLMN from a commercial operator in its home country or in a foreign country.

In LTE, two models are defined for roaming:

- Home routed roaming,
- Local break-out roaming.

The two models have different implications in terms of architecture and traffic control that are further described hereafter.

4.1.4.1 Home routed roaming model

Diameter is an Authentication Authorization and Accounting (AAA) protocol. It works at the OSI Application Layer, and is used as default technology in cellular system. The home routed model requires a roaming agreement, interconnection between networks with security features such as Diameter Edge Agent (DEA) and interfaces between networks such as S6a (for signalling for authentication), S8 (user plane), S10 if there is mobility.

Figure 7 shows the home routing model. Using the home routed model, the subscriber data traffic is served by the Home Network PGW. This model gives the home PLMN more control on the PPDR user traffic (charging, DPI, Lawful intercept...). Policy and Charging are handled in the home network. This model is the one which is the most popular in commercial world today.

With this model, the PPDR user experience remains similar as if at home. Besides, it allows to access securely to PPDR applications.

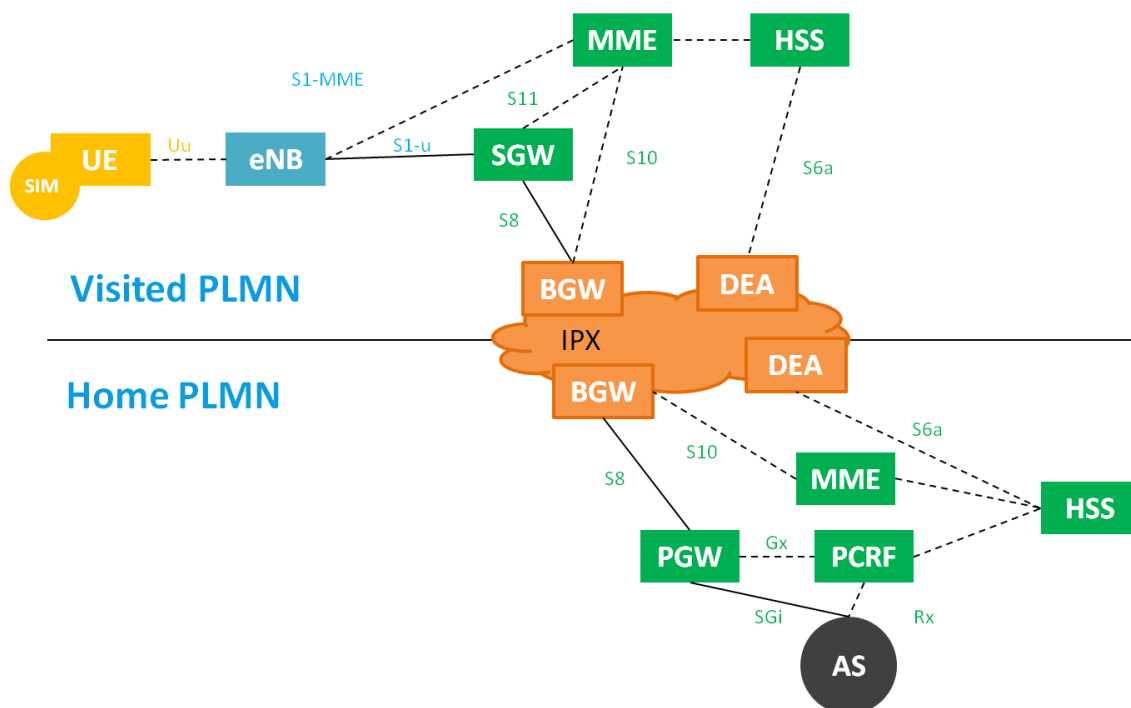


Figure 7 – Home routed roaming model (simplified – charging not depicted-)

It is to be noted that the traffic between the two networks must rely on IPX (IP Exchange) network which is an evolution of GRX networks used in previous 2G/3G systems for data roaming. IPX is a dedicated and secured roaming / interworking network to interconnect home and visited networks. The DEA acts as a single entry point for the signalling traffic.

4.1.4.2 Local breakout roaming model

Figure 8 shows the local breakout model. This model has a different architecture with new interfaces S9 (Diameter based) used to transfer (QoS) policy and charging information between the Home PCRF and the Visited PCRF.

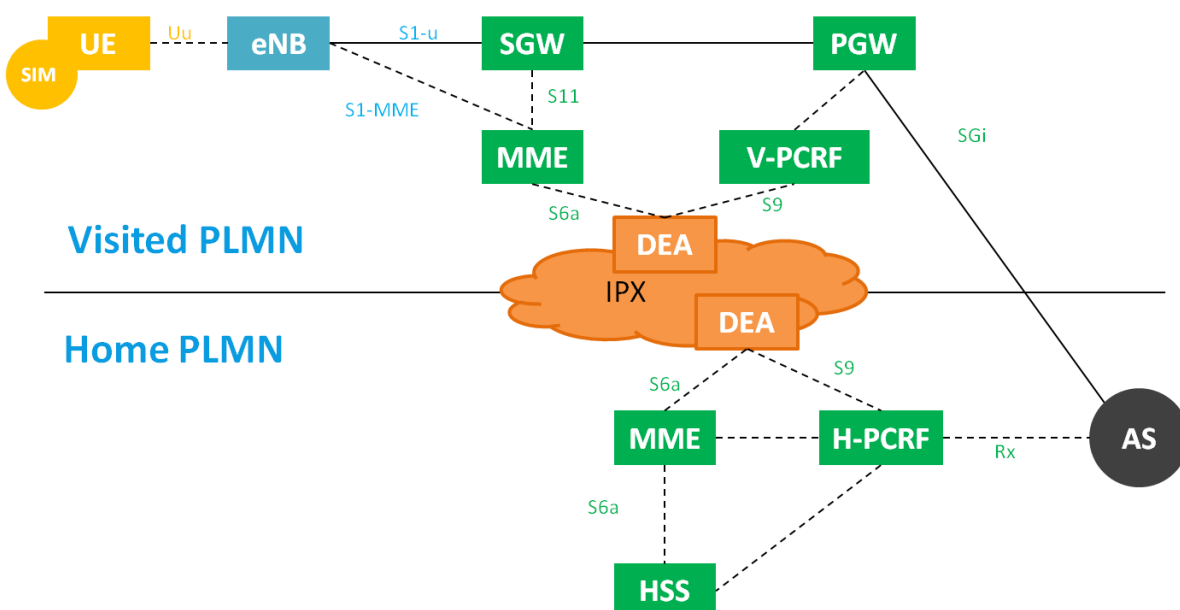


Figure 8 – LTE local breakout architecture (simplified – without charging)

In this case, the end-user data traffic is served by the Visited Network. This may allow for more efficient routing (in terms of bandwidth, latency, less delay) and eventually lowers cost of transport (especially in case of roaming to a foreign country). However, if the PPDR user roams, he still may want to access securely to the user's local applications and then the previous advantages do not apply anymore. It may be noted that the visited PLMN has full control over the visited PGW and PCRF, therefore the user experience depends on the capabilities of the visited network (the visited PCRF enforces the QoS policies to the home PCRF via the S99 interface).

This model requires high-level of alignment of network architecture and interface definition (3GPP releases, fields, content) and, Authentication, Policy, and Charging must be done in cooperation.

4.2 IEEE 802.11 specific Quality of Service mechanisms

IEEE 802.11 or WLAN is part of the overall solution in at least two ways. WLAN can be part of the infrastructure. Such solution is interesting in hotspots. WLAN can be used as a capacity extender, which is referred to as WLAN-offloading. This can be the case in sports arenas, dense urban areas, shopping malls, office buildings and other hotspots. The WLAN system can be part of the operators own system, in which case the WLAN is considered a “trusted” network. The WLAN system can also be external to the operators system. In such case, the WLAN system can still be part of the overall architecture. Such WLAN system is however considered as “untrusted”. The main difference between both options relates to security aspects of the system.

WLAN can also be used for creating ad-hoc (mesh) networks. Ad-hoc networks are self-organizing networks consisting of equal peers that can communicate without the need for central nodes. Networks without connectivity to an infrastructure that can auto configure completely are considered ad-hoc networks. Mesh networks are networks that can multi-hop. Some mesh networks may be preconfigured. In the scope of this document, mesh networks are ad-hoc networks in the sense that they can auto-configure.

Section 4.2.1 describes the QoS mechanisms for (infrastructure based) IEEE 802.11 hotspots. Section 0 describes the QoS mechanisms for ad-hoc networks, not yet considering the integration with an infrastructure. Section 4.3 describes how the combination between WLAN, ad-hoc and infrastructure QoS mechanisms could be realized.

4.2.1 Quality of Service mechanisms in hot spot systems

A key element to the 802.11 performance success is its simple MAC operation, based on the DCF protocol. This scheme has proven to be robust and adaptive to variable conditions, able to cover most of the needs. The available data rate was sufficient for the best effort applications, so complex resource scheduling and management algorithms were unnecessary. However, with the recent growth of multimedia applications, such as voice and video streaming, different demands for QoS are created. Therefore, traffic differentiation and network management have become inevitable to support more demanding applications.

With the purpose of enhancing the WLAN standards for supporting QoS, the 802.11e amendment was established. This amendment tries to deal with the several challenges to provide QoS, as summarized in Table 5.

Table 5 – Challenges in providing QoS in IEEE 802.11e

Challenges	Issues	Effects
Managing link layer resources	- Access coordination; - Parameter settings; - Admission control.	- Throughput degradation; - Inefficient resource usage; - Poor QoS differentiation.
Handling time-varying network conditions	- Retransmissions; - High collisions; - Large defer periods.	- Throughput degradation; - Priority inversion; - Starvation.
Adapting to varying application profiles	- Dynamic demands; - Unknown traffic profile; - Static scheduler.	- Unacceptable delays; - Buffer overflows; - Resource inefficiency.

The 802.11e provides a new MAC scheme, the Hybrid Coordination Function (HCF), which presents two MAC protocol versions with centralized and distributed control. The first one for centralized control is implemented by HCF Controlled Channel Access (HCCA), an improved variant of the PCF, requiring a central coordination instance that schedules medium access. The second one for distributed control is an Enhanced Distributed Channel Access (EDCA).

Other improvement of the 802.11e amendment is the Direct Link Protocol (DLP). The legacy standards do not allow a station to directly transmit frames to another, within the infrastructure BSS, all the communications between two stations have to go through the AP. With DLP introduced for QoS-enhanced station to setup the direct communication between each other in the infrastructure mode, which can significantly increase the bandwidth. The following Figure 9 illustrates the HCF control framework.

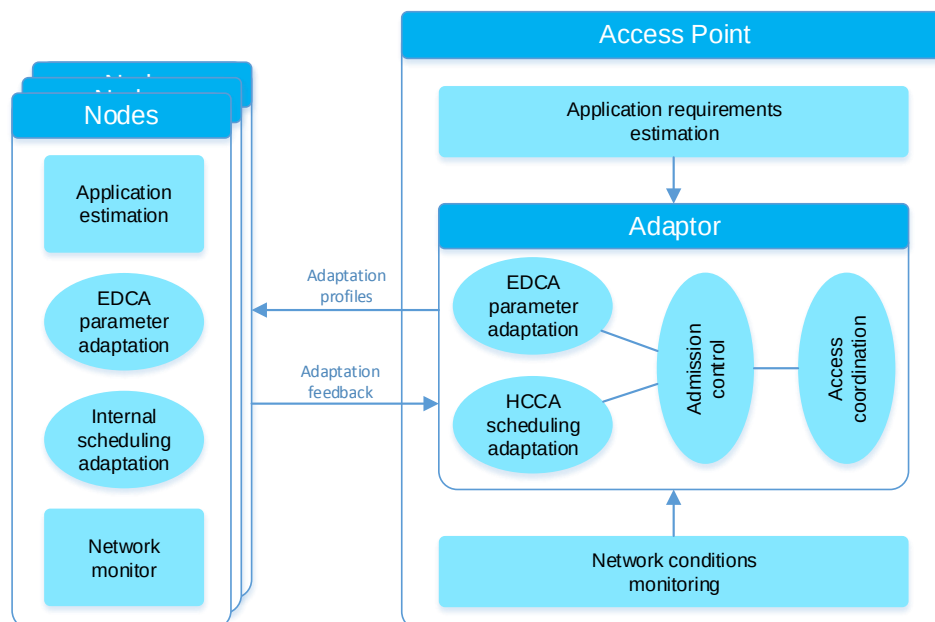


Figure 9 – HCF control framework

While DCF does not differentiate between traffic with different QoS needs, EDCA supports four traffic categories: voice, video, best effort, and background, with different rules to access the

wireless medium to support the user priorities defined in IEEE 802.1D. The mapping between the user priorities and the traffic categories of EDCA is illustrated in Table 6 and Figure 10.

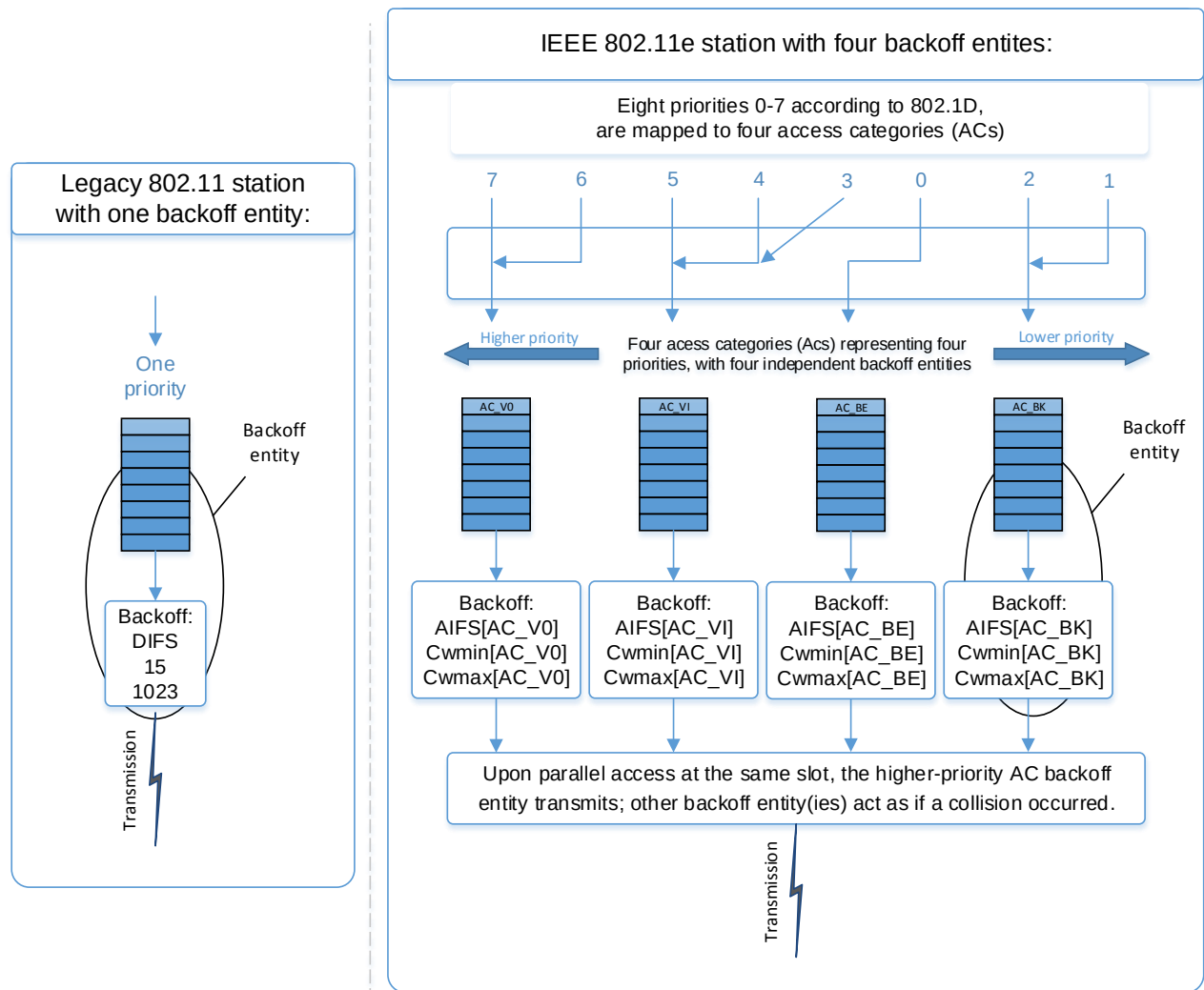


Figure 10 – Legacy 802.11 station and 802.11e station with four ACs within one station

Table 6 – Mapping between User Priority and Access Category

User Priority (Same as 802.1D)	802.1D Designation	802.11e AC (Access Category)	Service Type
2	Not Defined	0	Best Effort
1	Background (BK)	0	Best Effort
0	Best Effort (BE)	0	Best Effort
3	Excellent Effort (BE)	1	Video Probe
4	Controlled Load (CL)	2	Video
5	VI (Video <100ms latency and jitter)	2	Video
6	VO (Video <10ms latency and jitter)	3	Voice
7	Network Control (NC)	3	Voice

EDCA prioritizes traffic categories by different contention parameters, including arbitrary inter-frame space, maximum and minimum back off window size (CW_{max}/min), and a multiplication factor for expanding the back off window. Although all traffic categories keep using the same DCF access method, they have different probabilities of winning the channel contention by differentiating contention parameters. EDCA allows any combinations of these contention parameters according to the service provider's needs.

4.2.2 Quality of Service mechanisms in ad-hoc networks

Mobile ad hoc networks (MANETs) are distributed systems comprising wireless mobile nodes that can self-organize dynamically into arbitrary and temporary, ad-hoc network topologies. Starting point for the definition of QoS mechanisms in ad-hoc networks is the foreseen use of the ad-hoc network function in the PPDR application domain.

Ad-hoc networks imply that each device that is part of the ad-hoc network can be an intermediate node forwarding the data of other devices. As a result, being part of an ad-hoc network requires capable devices. The device will consume more energy due to the additional processing and the additional transmissions. And devices need to be able to receive and transmit over different interfaces simultaneously. It is important to distinguish between end-point devices and router devices. Handheld devices (terminals) are battery powered. Using such devices for relaying data should be considered only as a last resort, to avoid battery drainage. As a result with respect to QoS, such devices are clients. Router devices however are designed to relay data.

Since mobile devices are free to move randomly, the MANET's topology may change rapidly and unpredictably [12]. The above distinction, limits this. The 'real' mobile devices are the handhelds. Router devices have a more nomadic behaviour being mounted on board of e.g. vehicles. As such they create an ad-hoc infrastructure for the handheld devices. For the design of QoS in ad-hoc networks nomadic behaviour is therefore assumed. In general, communication in a mobile ad hoc network can occur directly between mobile nodes or through intermediate nodes acting as routers. For PPDR services the ad-hoc network itself is an intermediate medium to connect mobile devices either to one another or with the infrastructure.

Minimal configuration and quick deployment make mobile ad hoc networks suitable for emergency situations like natural, technical or man-made disasters, military conflicts, emergency medical situations, etc., where the wired network is not available and mobile ad hoc networks can be the only viable means for communications and information access.

In order to provide high quality communication, the QoS mechanisms in the ad-hoc network must be able to handle the following key characteristics/uncertainties:

- Node-to-node radio conditions vary, which implies that the achievable bandwidth between nodes vary. This includes also interference from outside the system, as in most cases, the ad-hoc network shares the spectrum with other users.
- It is a distributed network. No central control with full view of the conditions exists.
- It is in potential multi-hop communication, the QoS must be established end-to-end.
- The traffic consists of different traffic classes and different priorities.

This section proposes some basic ideas on how QoS in ad-hoc networks can be realized. First this section providing a QoS framework. Next this section introduces a possible protocol to implement this.

4.2.2.1 Quality of Service in Ad-hoc Networks

Ad-hoc networks will need to increase their usability by providing correct traffic differentiation, supporting heterogeneous services and supporting applications which require QoS provisioning. Many applications are usually delay sensitive and therefore the end-to-end delay has to be below a certain limit. Although, QoS has been improved in ad-hoc networks, there are some challenges such as lack of centralized control, limited transmission range, high mobility, battery and computational power constraints that have not yet been solved. In a multi-hop ad-hoc network, QoS provisioning is affected by challenges in the physical, data-link and network layers.

Communication over the wireless medium is susceptible to fluctuations in the radio channels and factors such as interference, fading and noise may lead to lower bit rates or higher bit error rate (BER). The mobility of nodes within an established network introduces unpredictable link failures which often result to reconfiguration. Additionally, mobile nodes are usually limited by the battery power where the transmit power of devices is a function of the power consumption and this affects the QoS attributes. To assure a proper QoS at the physical layer, a dynamic control of the wireless link is needed. Factors such as the transmission power, signal-to-noise ratio (SNR), receiver sensitivity and transmission rate can directly influence the QoS metrics.

The data link layer which consists of the Medium Access Control (MAC) and the Logical Link Control (LLC) sub-layers is responsible for establishing and maintaining physical and logical communication between nodes. The MAC sub-layer is responsible for most of the issues relating to QoS provisioning, this includes traffic differentiation, resource reservation, the problems of hidden and exposed nodes, and efficient and fair channel access. An ideal MAC protocol should be able to efficiently share available resources between nodes, achieve high throughput and support different traffic classes and the associated QoS requirement. The problem of QoS support at the MAC layer is being an active research area in recent years with the IEEE 802.11 EDCA [13] protocol being a prime commercially available QoS MAC protocol.

The mobility of node in a random and unpredictable manner severely affects the network topology and routing protocols have to adjust accordingly. Additionally, signalling protocols would be required for admission controls, resources reservation and negotiation of QoS parameters. All the above mentioned features make QoS provisioning in ad-hoc network to be a challenging task. The provision of adequate QoS for multi-hop ad-hoc network requires the interaction between the physical, data link and network layers. Interactions between the physical and data-link layer may be sufficient for single-hop communication, however, for multi-hop communications a comprehensive cross layer approach may be needed.

4.2.2.2 Cross Layer QoS Architecture

A cross layer approach to the guaranteeing of QoS provisioning in multi-hop ad-hoc network will involve the integration of singular efforts at different layers of the ISO/OSI model into one complete approach. An advantage of using such cooperative mechanism is the ability to share relevant information between layers and provide feedback between components in the architecture. This will also contribute to adapting to the dynamic nature of MANET environment. A disadvantage of the cross layer approach lies in the associated overhead with the control signalling and feedback loops. The cross layer approach gives more design flexibility and most of the proposed architectures have many similarities and have significantly influenced each other. Prominent architectures which have influenced others and relevant to the scenarios considered with the SALUS project such as the INSIGNIA, SWAN, DAIDALOS and HQMM are

described below. Table 7 shows the important building blocks of a cross layer architecture and most of the blocks are present in the discussed architecture.

Table 7 – The basic building block of a cross layer approach

ISO/OSI Layer	Building blocks
PHY	Channel monitoring (rate, SNR, BER), dynamic rate control
MAC	Bandwidth estimation, priority queuing, traffic differentiation
Network	QoS routing, QoS signalling (resource reservation), traffic classification, traffic shaping, admission control

4.2.2.3 INSIGNIA

The INSIGNIA QoS framework operates mainly in the IP layer and is designed to support multimedia services. It aims to support either base QoS or enhanced QoS depending on the available resources. Figure 11 presents an overview of the architecture of INSIGNIA. The admission control allocates bandwidth to flows based on information provided by the service, thereby allowing either the base or enhanced QoS. The decision to admit a flow to the network is based on criteria such as requested bandwidth, measured channel capacity and the current channel utilization. Admission control is implemented on a hop-by-hop basis; each intermediate node upon receiving a reservation packet decides to accept or denies the request. Scheduling is performed in INSIGNIA in a weighted round robin manner and in-band signalling is used for establishing, adapting, restoring and tearing down end-to-end QoS sessions. Within this framework, neither the routing nor MAC protocols are defined; however, INSIGNIA can be used with already existing protocols.

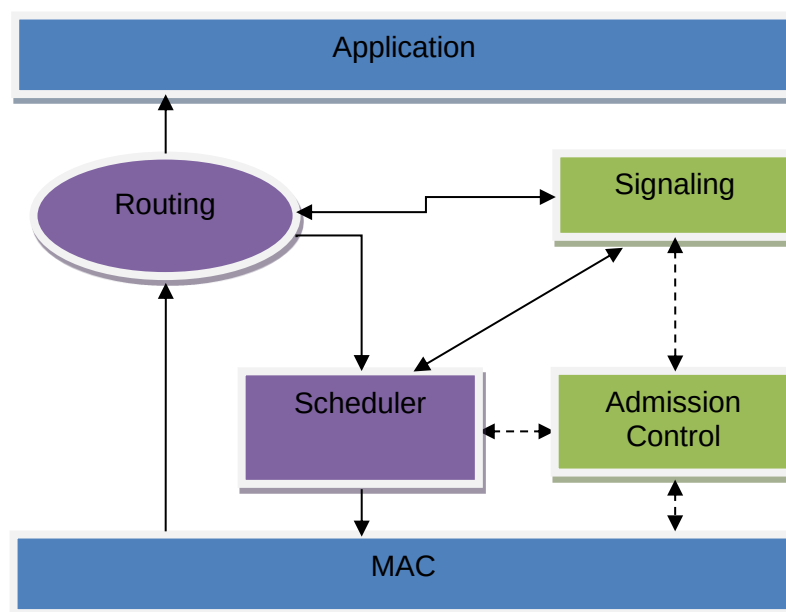


Figure 11 – The INSIGNIA architecture (adapted from: [14])

4.2.2.4 DAIDALOS approach

This QoS framework was developed within the DAIDALOS research project [15] and was further developed during the DAIDALOS II project [16]. The DAIDALOS approach aims to provide a cross layer solution to integrate ad-hoc networks with infrastructure network. This is an ideal situation within the scenarios considered in SALUS project. This architecture supports MAC layer service differentiation for the four IEEE 802.11 EDCA (Enhanced Distributed Channel Access) access categories. The end-to-end signalling allows resource reservation to come from either the ad-hoc or the infrastructure part. The ad-hoc signalling mechanism is integrated with the Next Step in Signalling (NSIS) protocol in the infrastructure network.

This architecture is capable of providing MAC layer measurement, dynamic regulation with admission control and traffic shaping and also featured the first real life implementation of EDCA in a MANET [19]. The ad-hoc part of this QoS architecture consists of two main logical units, the mobile node (MN) and the gateway (GW) as shown in Figure 12. MN functions as both a user terminal which provides QoS support to the end user and as a router which forwards the traffic of neighbouring nodes. The physical interaction between the MANET and the infrastructure planes occurs at GW. The GW provides connectivity with infrastructure, participates in admission control and dynamic regulation. It is also responsible for the interaction of QoS signalling. End-to-end QoS resource management is supported more specifically through the interoperation of the QoS Client (QoSC) in the MN and QoS Manager (QoSM) in the GW. The QoSC retrieves the necessary QoS parameters from applications (through an API) and maps them to network QoS parameters.

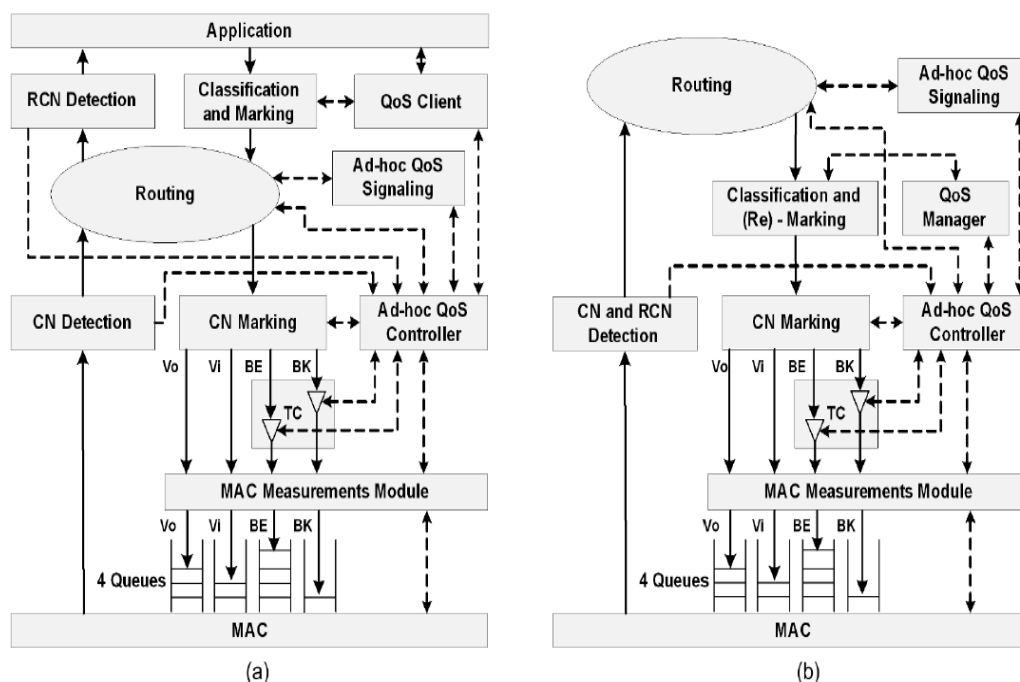


Figure 12 – DAIDALOS Architecture for (a) mobile node and (b) gateway (obtained from: [16])

The Ad-hoc QoS Controller (AHQoSC) manages the work of the other modules, collects information about available resources in the wireless medium, and performs admission control and traffic control in the ad-hoc path. The MAC Measurements Module (MMM) provides AHQoSC with information regarding bandwidth utilization, transmission delay, frame statistics, current transmission rate and idle intervals. The Ad-hoc QoS Signalling (AHQoSSig) module

performs the QoS negotiations, probing for available bandwidth and session setup between infrastructure and ad-hoc. The Traffic Controller (TC) module together with the IEEE 802.11 ECDA function performs the traffic differentiation. The architecture is aware of overload situations through the Congestion Notification (CN) signalling mechanism, which is implemented in three modules: CN Marking (CNM), CN Detection (CND), and Receiver CN Detection (RCND).

4.2.2.5 SWAN Model

Another important distributed cross-layer QoS framework that has been used in MANETs is called Stateless Wireless Ad-Hoc Networks (SWAN) [17]. The main advantages provided by this framework include:

- QoS negotiation
- Service differentiation
- Dynamic regulation in case of congestion
- Admission control

SWAN considers 2 traffic classes; best effort traffic and real time traffic. A general overview of its architecture is shown in Figure 13.

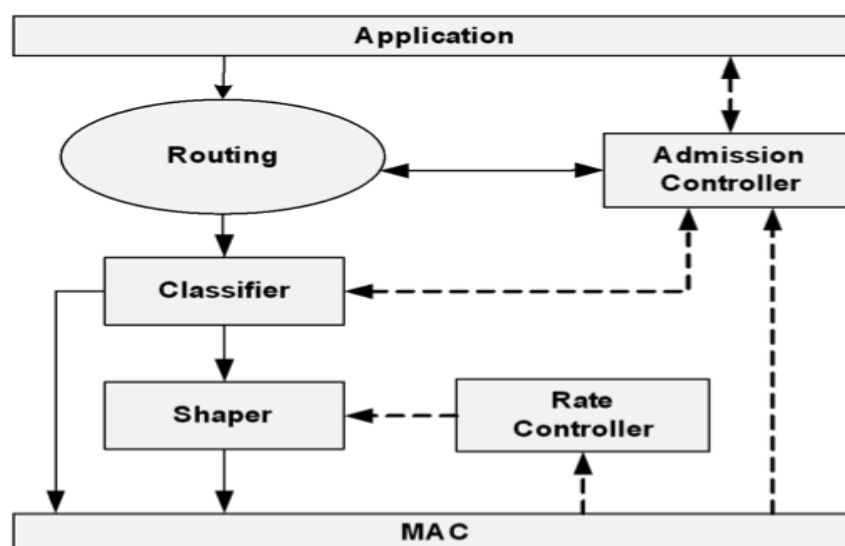


Figure 13 – SWAN architecture (Obtained from: [17])

All nodes include multiple mechanisms, which exist in the SWAN model. The traffic between the aforementioned classes is differentiated by the classifier and packets are marked accordingly. The process of differentiation can be achieved since real time packets are forwarded directly to the MAC layer and best effort packets go directly to the shaper. The role of the shaper is to delay packets according to the calculated rate by the rate controller. Delay measurements in the MAC layer contribute to the rate controller operation. Another characteristic of SWAN is that it is stateless, so each intermediate node does not maintain any aggregate or per flow state information.

The admission control is performed exclusively by the source, thus estimation of the available bandwidth is required. The calculation of the available bandwidth is provided by the admission controller. During this process request and response, probes are sent to the destination in order to calculate the bottleneck bandwidth in the path. Then a decision is made according to the

received information. The packets are treated as real time packets by the classifier if the session is admitted; else they are marked as best effort packets.

In case of congestion, dynamic regulation of real time sessions has to be performed. Congestion is caused by dynamic rerouting and mobility of the nodes. By the time a mobile node identifies a violation of the real time traffic utilization limits, and then it marks explicit congestion notification bits in the IP header of the real time packets. Hence, the source node can be informed about the congestion by the destination node, which monitors incoming packets, by receiving a regulated message. Then, the source node sends a new probe request to the destination so as to establish the real time session again. The outcome of re-establishing the real time session is either to achieve the previous quality of service or to drop the session. The SWAN model does not consider bandwidth adaptation of real time sessions.

4.2.2.6 HQMM Model

The Hybrid QoS Model for Mobile Ad Hoc Networks (HQMM) [18] is a combination of the DiffServ and IntServ models that are described on the next page. According to this model, per-flow provisioning, which is based on INSIGNIA model, is given to traffic that has the greatest priority. Per-class provisioning, which is based on DiffServ model, is given to other priorities. The HQMM model uses three different node types:

- i. Ingress nodes
- ii. Interior nodes
- iii. Egress nodes

Figure 14 illustrates the node architecture, which is the same for all nodes, since each of them can perform all of these functions, even at the same time.

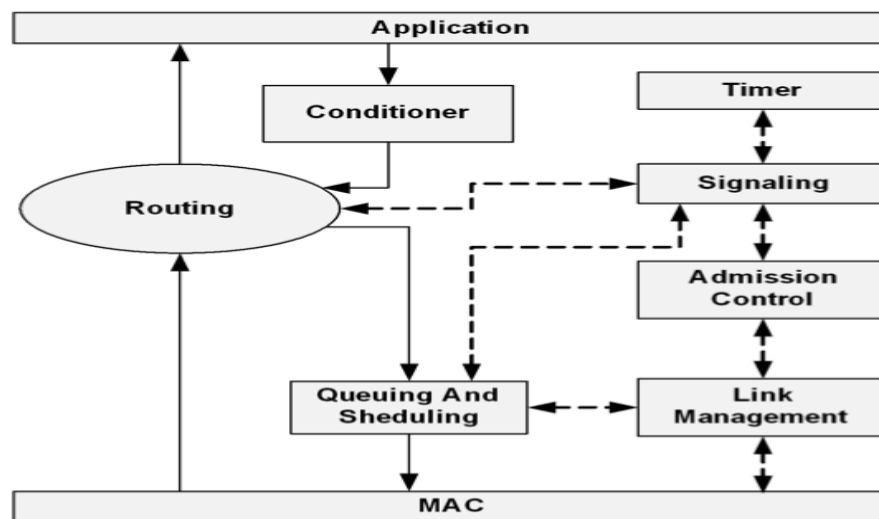


Figure 14 – HQMM Architecture (obtained from: [18])

The choice of routing protocol is out of the scope of the HQMM model. The signalling block operates in a similar way to the signalling block of the aforementioned INSIGNIA model. Then, the link management block monitors the wireless channel in order to report the average and the current available bandwidth. Queue management algorithms, scheduling and packet classification help to fulfil service differentiation. Above all, every INSIGNIA reservation packet is treated with the highest priority compared to each other packet, which is put in DiffServ classes.

Typically, there are two different models that QoS revolves around and these are listed below:

- DiffServ: This model differentiates the delivery of aggregate traffic classes. It is simple in deployment.
- IntServ: This model provides strict per flow guarantees, but requires supplementary implementation and is complex in deployment.

QoS is assured by using two principal approaches defined at the MAC layer. The first approach, used in most of the cases, is the prioritized approach and is based on the DiffServ model. In this approach, violations of QoS are permitted over limited time periods, but the session requirements of QoS are held during the total transmission time. The second approach, named parameterized approach, based on the IntServ model has strict requirements which can be expressed in terms of quantitative values (e.g. delay bounds, jitter, data rate, etc.).

QoS provisioning is basically relied on various parameters known as performance metrics. Some of the common QoS metrics include:

- Maximum frame delay: The time period that a frame has to wait at the MAC layer until its transmission is successful. It is measured in seconds.
- Minimum throughput: It is the amount of data that a single station can transmit through a wireless channel per the time period. It is measured in bits per second.
- Maximum frame loss ratio: It is maximum number of tolerable fractions of frames that can be lost at the MAC layer. It is measured in percent.
- Maximum variation of frame delay or jitter: It is the difference of the upper bound of frame delay and the minimum delay. The upper bound frame delay includes MAC queuing and retransmissions delays, and the minimum delay includes frame transmission delay.

4.2.2.7 Issues affecting QoS Provisioning

Although mobile ad-hoc networks have important advantages, some of their characteristics cause problems when meeting QoS requirement for various applications. The most common issues are listed below.

Issues based on Technology:

- Multiple channels: The complexity of MAC protocols increases, when nodes are equipped with more than one wireless interface.
- Directional antennas: The use of directional antennas on stations can lead to reducing the interference and increasing the performance of the transceiver, but at the same time this can create hidden stations causing detrimental result on QoS.

Issues based on Deployment:

- Limited battery power: Stations within mobile ad-hoc networks use batteries for their energy supply. Hence, MAC protocols should keep transmissions power levels to a minimum, reduce retransmissions and employ power saving. All these facts have to be addressed without sacrificing QoS.
- Mobility: The continuous movement of stations often leads to link breakage, collisions and variation in the number of contenting stations. For the alleviation of these problems, traffic control mechanisms can be defined.

- Limited computational power: The computational power of mobile devices is limited and therefore highly complex algorithms cannot be used by MAC protocols to guarantee QoS.

Inherent Issues:

- Limited reliability of the wireless channel: The quality of radio channels is affected by thermal noise, multi-path fading, interference, shadowing and the near-far problem. Therefore, the poor performance of radio channels can lead to retransmissions and varying transmission rates which affect QoS.
- Applications requirements: Plenty of the requirements of the applications have to be fulfilled by the QoS MAC protocols.

4.2.2.8 QoS-aware Routing

The routing of real-time and multimedia data packets in MANETs is key towards its deployment in critical, emergency and tactical military communication scenarios as described in some scenarios for SALUS. Thus, there is a requirement for routing approaches to provide the required QoS guarantees that are usually measured in terms of throughput, end-to-end delay, delay jitter and packet loss rate.

However, due to the highly dynamic wireless network state, the task of ensuring hard QoS routing guarantees is a non-deterministic polynomial time (NP)-Complete problem for MANETs [20]. Therefore, most of the techniques designed for traditional networks are not applicable to MANETs due to the unique challenges imposed by such networks [21].

The Integrated Service (IntServ) and Differentiated Service (DiffServ) QoS models used in traditional networks are applicable to routing protocols. IntServ provides QoS for each flow of data in the network creating a virtual connection-oriented path where specific state information has to be maintained for every flow in all intermediate nodes including bandwidth requirements and other QoS measurements. The DiffServ model aims to provide scalable service differentiation, without maintaining per flow state information and signalling at every intermediate node so that a service model for aggregated traffic classes supporting QoS is provided. There is no explicit signalling in the network (i.e. the routers) before data transmission. Instead, the network tries to deliver a specific service based on the QoS specified by each packet.

4.3 Conclusion on Quality of Service solutions towards unification for an integrated solution

The information on this subsection has been considered security sensitive and it has been moved to D6.1 RESTREINT EU Annex, which is a separated document (SALUS_D6.1_Annex_v1.0.docx)

5 MOBILITY MECHANISMS

The SALUS PPDR system is actually a system of systems. It will contain of TETRA, TETRAPOL, LTE, WLAN hotspot and ad-hoc networks. This combination of systems serves a variety of purposes. This includes continuity in coverage and reliance of the overall system, maximizing reliability.

In SALUS all services can be carried by IP. When availability of the service can only be realized by moving from one radio system to another, the SALUS system should support that the service continues seamlessly. i.e. the end-user should not notice the handover, or at the most notice the difference in supported bandwidth. As all services are carried by IP, continuity of the IP stream during mobility creates continuity of the service

5.1 IP-layer mobility

For IP-layer mobility SALUS will use the fast handovers for Proxy Mobile IPv6 (PFMIPv6) standard [22] extended with support for multicast listeners. Fast handovers is an extension for Proxy Mobile IPv6 (PMIPv6) [23] that allows for seamless handovers between devices within a PFMIPv6 domain. IPv4 support is available in both PMIPv6 and PFMIPv6 [24].

This standard allows users of the PPDR network to switch between access networks of the same or different technologies without losing connection or IP address.

5.1.1 Mobility Architecture

The IP mobility system connects the different mobile access methods of the PPDR network to the PPDR core network and external networks to the PPDR network. An overview of how SALUS thinks such a network should look can be seen in Figure 15. In a straightforward solution each network has its own Mobile Access Gateway(s) (MAG(s) and the entire network should have a single Local Mobility Anchor (LMA). These concepts will be explained in section 5.1.2. This would mean that there will be one or more MAGs per PPDR location (for example a police station), but also a single MAG for an entire LTE network. This last situation is not preferable but putting the MAGs in the actual LTE network is most likely not feasible in the short term (it could however be a long term goal).

One of the goals of the SALUS is that devices can also connect to the PPDR network via a public network. It is proposed that devices not connected to the SALUS network have the ability to connect to it using a tunnelling solution. This tunnel would be set up between the device and a special MAG that acts as a tunnel endpoint ("External MAG" in Figure 15). Using a secure tunnel will also increase the security of information as it could travel over the public internet in this situation.

The Control Center is an entity that can control the network and the MNs connected to it, for example assigning talk groups to different Mobile Nodes (MNs). The Information Database should contain information relevant to MN mobility, such as the location of different mobile networks and which MAGs are responsible for them.

Initially we propose the system to be purely IPv6 based. This will simplify the initial deployment as IPv4 is only supported in PMIP (Proxy Mobile IP) systems using an extension. Multicasting

has also received some improvements in IPv6 that could potentially simplify an initial demonstration deployment of the SALUS system.

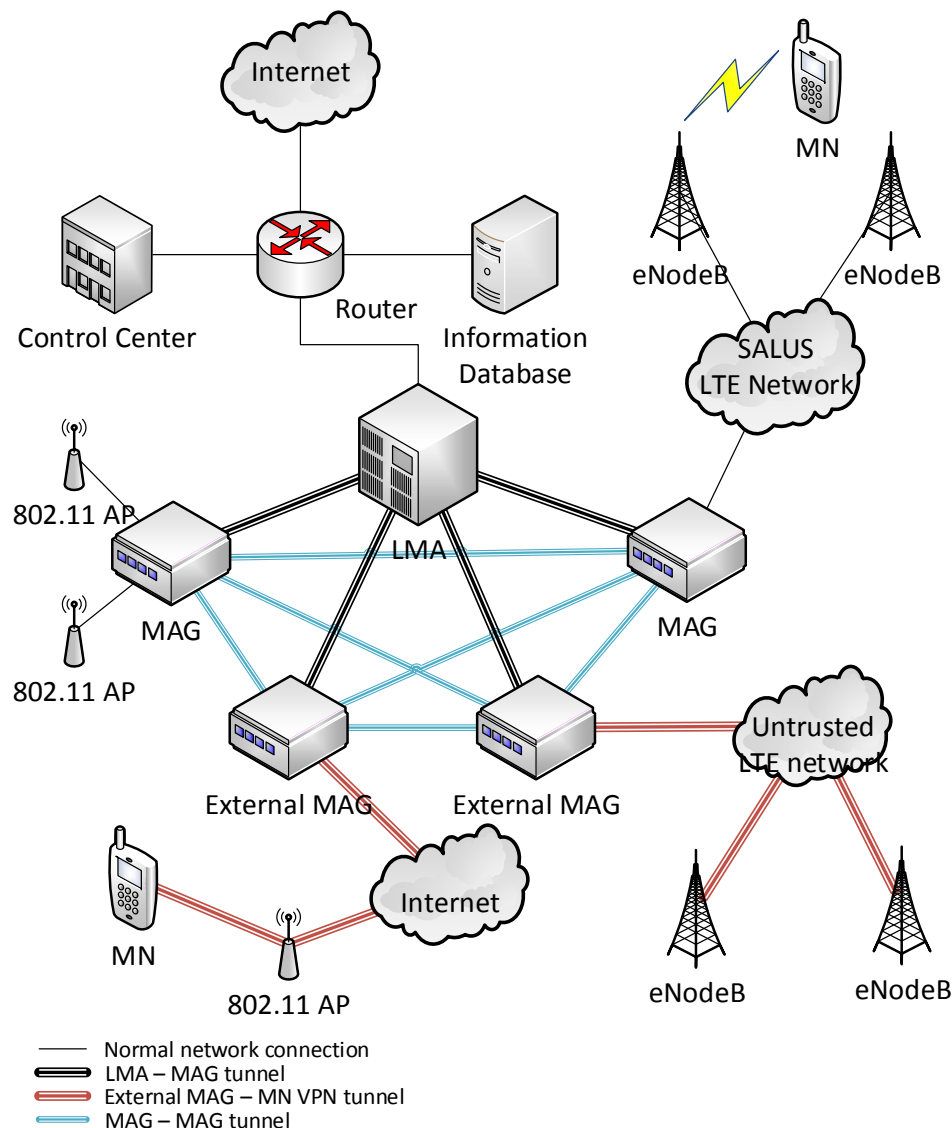


Figure 15 – SALUS architecture proposal

Under such approach MNs/UE will be free to roam from one location's IEEE 802.11 network to the SALUS LTE network and back to another location's IEEE 802.11 network without noticing a change on the IP layer.

5.1.2 Proxy mobile IPv6

Proxy Mobile IP (PMIP) adds two new network nodes to an IPv6 based network: The Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA is the anchor point for the Mobile Nodes (MNs) in the Proxy Fast Mobile IPv6 (PFMIPv6) domain (All IP routes from the greater internet towards the MNs lead to the LMA). A PMIPv6 domain can have one or more LMAs, were different MNs can be assigned to different LMAs. The MAG acts as the first hop router for the MN. An overview of this setup can be seen in Figure 16. Once a MN connects to a PMIPv6 network the MAG it is connected to will send a Proxy Binding Update (PBU) message to the LMA containing information about the MN relevant to the mobility operation. The LMA will acknowledge with a Proxy Binding Acknowledgement (PBA) message. The MAG will send IPv6

router advertisements that the MN will use to obtain an IP address using IPv6 auto-configuration. All traffic will be tunnelled between the MAG and LMA, giving the perception that the MN is actually located within the IP network the LMA resides in independent of the network the MN and MAG actually reside in. The MAG can be positioned in the foreign network (for example a LTE network) or act as an attachment point for a network (if the network provides its own mobility management internally).

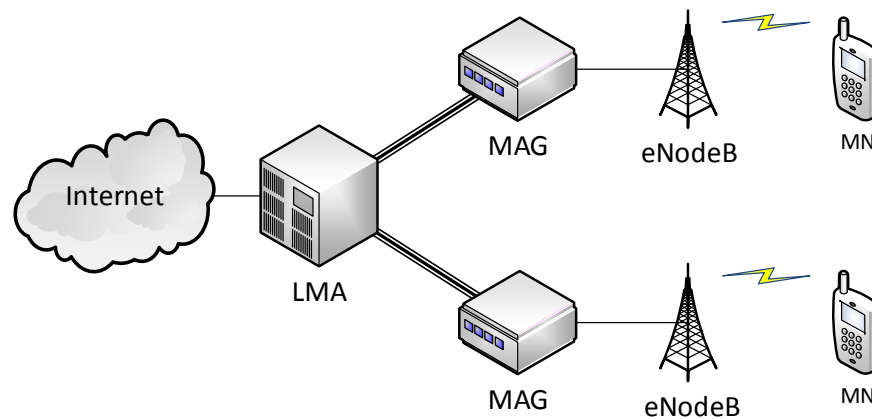


Figure 16 – Proxy Mobile IPv6 architecture

A MN can change its point of attachment freely between networks with a MAG and always keep the same IP address as it would have on its home network. All MAGs will have the same link layer address as seen from the MN. As a result the MN does not know that it is actually on a different link and keeps the same IP address (If the MN requests a new IP address it would also receive the same one it had before).

While PMIPv6 is mostly focussed on providing IPv6 mobility it is also possible to extend this with IPv4 support if needed. This extension allows IPv4 connectivity between the MN and the IP network the LMA is in. It does not provide support for using PMIP over an IPv4 network. Proxy Mobile IP is also an optional part of the 3GPP LTE specification, in which it replaces the GRPS Tunnelling Protocol (GTP) when used.

5.1.3 Fast handovers for proxy mobile IPv6

Fast handovers for Proxy Mobile IPv6 (PFMIPv6) adds seamless handovers to the PMIPv6 system. A MN can switch its point of attachment to another network and have no packets sent to it lost during the handover. The handover should also perform significantly faster than without fast handover support.

Seamless handovers are made possible by changing the handover procedure in the MAG (The LMA is not changed) compared to normal PMIPv6. The PFMIPv6 protocol covers two handover situations:

1. Predictive handover
2. Reactive handover

The predictive scenario is illustrated in Figure 17. The handover preparation starts by the network or MN itself predicting the movement of the MN (The MN needs to report link layer information to the network for this, possibly by using Media Independent Handover (MIH) and signalling this information towards the MAG (1 and 2). The network then initiates a handover when it thinks the MN is moving towards a new MAG. The Previous (current) MAG (pMAG)

sends a Handover Initiation message (3) to the New MAG (nMAG) which responds with a Handover Acknowledgement (HACK) (4). A tunnel is set up between the pMAG and nMAG to forward data for the MN that arrives at the pMAG to the nMAG. The nMAG buffers this data until the MN is connected. The pMAG now orders the MN to perform the handover (5). Once the MN connects to the nMAG the data that was buffered is sent to the MN. Data from the MN that is received at the nMAG before the LMA is updated is tunnelled back towards the pMAG to be send to the LMA. The nMAG finally updates the LMA with the MNs new location information using the normal PMIP signalling packets (6 and 7). This system allows the MN to handover quickly without packet loss as these are all buffered during the time the MN is disconnected from the network.

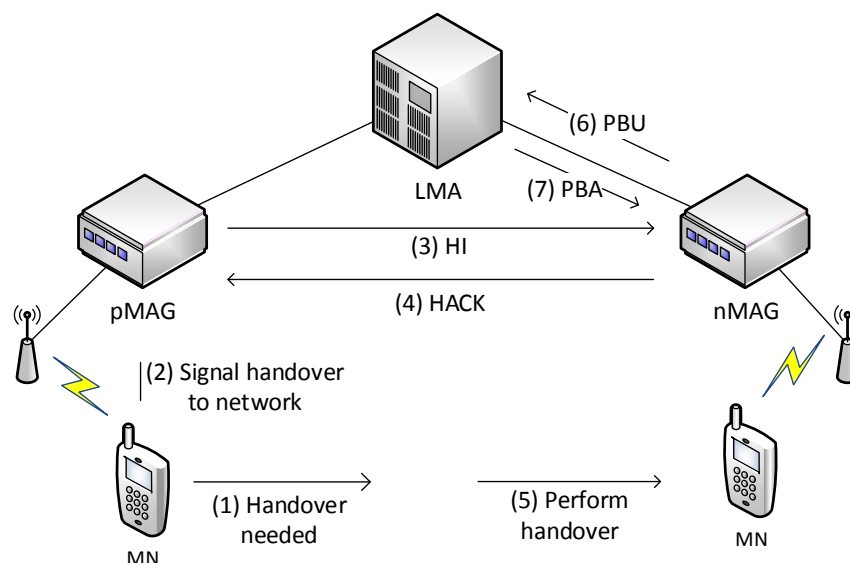


Figure 17 – PFMIPv6 predictive handover

In the reactive handover scenario the MN performs a handover without the network being aware of this beforehand. This situation can occur when the signal strength of the access point the MN is currently using suddenly drops. When the MN connects to the nMAG the nMAG will send a Handover Initiation message to the pMAG (It is left up to the implementation to decide how the nMAG learns about the pMAG). The tunnel can then be set up to allow messages still arriving at the pMAG to be forwarded to the nMAG. The nMAG then updates the LMA and the tunnel is discarded.

5.1.4 Multicast

Using multicast traffic for group communication will reduce the load on the network compared to using unicast traffic. MNs and other sources will only need to send a single packet to reach all interested destinations instead of sending a unicast packet to each destination independently.

Enabling multicasting within a PFMIPv6 domain is not straightforward, but the IETF working group on multicast mobility (Multimob) does have an experimental RFC on multicast sender support [25] and a draft for a listener extension in PFMIPv6 [26]. Both systems require a multicast proxy to be deployed on the MAGs and LMAs in the PFMIPv6 domain. The latter system also requires changes to the PFMIPv6 systems to signal fast handovers towards the nMAG. There is no standard (proposed or otherwise) for fast handover support for multicast senders yet.

5.1.4.1 Multicast proxies

The MAGs and LMAs need to be extended with multicast proxy functionality. The multicast proxy in the MAG will forward multicast group requests from the MN to the relevant LMA tunnel. The LMA in turn will forward this request to the multicast router it is connected to. The LMA will forward incoming multicast packets it has subscribed MAGs for to their respective tunnels. The MAG in turn will forward the packets to the downstream interfaces it has subscribed MNs on.

Proxy functionality is needed because normal multicast routing would disregard the LMA-MAG tunnels, leading to traffic being routed over possibly uncontrolled network connections. This approach also allows MNs to subscribe to multicast data available only in the private network. The fast handover systems also need to be extended to support multicast traffic. The HI message needs to be extended to include information about the multicast groups the MN is subscribed to. The nMAG can then already subscribe to these groups before the newly connected MN can send join requests. The multicast traffic for the MN is also tunnelled with the unicast traffic from the pMAG to the nMAG to prevent data loss in the time it takes to set up multicast traffic through the LMA-nMAG tunnel.

5.1.4.2 Relation between PMIP and MIH

To perform seamless handovers using the predictive handover mechanism the pMAG needs to be aware of two pieces of information:

1. That a MN is going to perform a handover
2. The MAG that is responsible for the target access network

How this information is obtained and signalled towards the pMAG is left to the PFMIPv6 implementation. There is also the possibility that the MN might need a trigger to perform the handover once PFMIPv6 has prepared the fast handover. The need for this functionality depends on the network and mobile device.

Within the SALUS project MIH is perfectly positioned to perform this signalling role. MIH can provide vertical handover services. MIH however needs to be implemented on all MNs involved and a large portion of the networking equipment. A MN or network device could signal the pMAG that the MN is about to perform a handover. The message would preferably also contain the IP address of the destination network MAG (the nMAG in this case). We believe that MIH could provide this mapping (Target network identifier - MAG IP address) as the system already contains information services for MIH devices. Figure 18 shows the most important devices from our viewpoint and which protocols (PFMIPv6 or MIH) they support. Note that we believe the MAGs should be the only point where PFMIPv6 and MIH interact with each other.

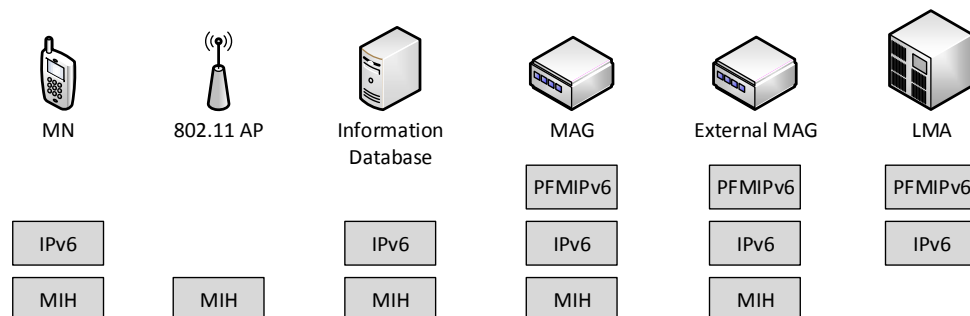


Figure 18 – Protocol overview

Figure 19 shows a situation in which a MN wants to switch to a different 802.11 AP which is on a different MAG. The handover could also be initiated from the network in which case the MN can be replaced with a network device. The message flow is an example of how this could work using MIH. The system that wants to initiate the handover queries an information database for the IP address of the MAG that serves the target access network (1) and gets a response (2). The handover initiating system then signals the current MAG of the MN with the handover command containing the IP address of the nMAG (3). This message is where MIH and PFMIPv6 meet. The MIH function on the MAG will now give PFMIPv6 the command to prepare the handover (4). Both MAGs now prepare the handover using normal PFMIPv6 signalling (5).

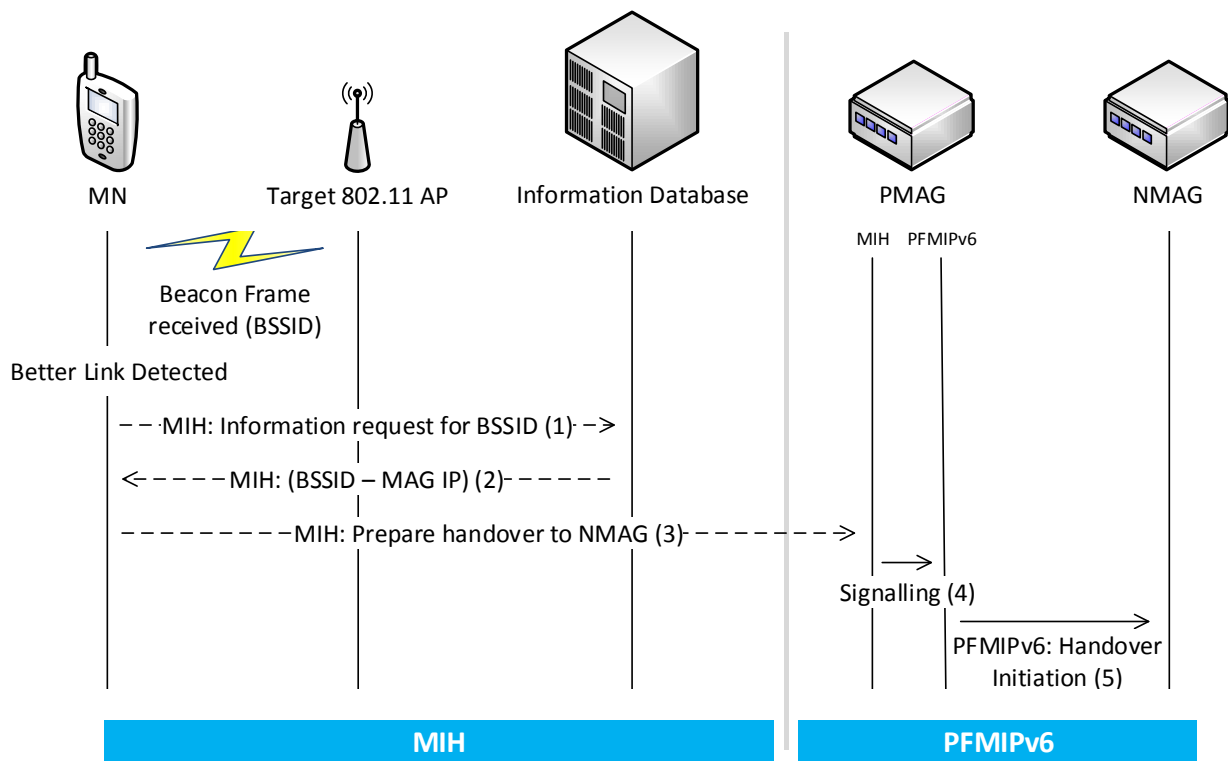


Figure 19 – Example of MIH signalling for PFMIPv6 handover

5.2 Media Independent Handovers

The Media Independent Handovers (MIH) standard is specified in standard IEEE 802.21 [50]. The main aim of this standard is to improve the user experience of mobile devices by facilitating handover between IEEE 802 networks whether or not they are of different media types, including both wired and wireless, where handover is not otherwise defined; and to make it possible for mobile devices to perform seamless handover where the network environment supports it. These mechanisms are also usable for handovers between IEEE 802 networks and non IEEE 802 networks (i.e. 3GPP Networks).

IEEE 802.21 provides link-layer intelligence and other related network information to upper layers to optimize handovers between heterogeneous networks. This includes media types specified by Third Generation Partnership Project (3GPP), 3G Partnership Project 2 (3GPP2), and both wired and wireless media in the IEEE 802 family of standards [50]. In this document we will focus mainly in 3GPP technologies (LTE) and IEEE 802.11 (Wi-Fi). IEEE 802.21 also defines new functional modules and concepts that should be added to the networks and devices (Mobile Nodes). Table 8 describes the main new concepts and modules within this standard.

Table 8 – Main concepts within standard IEEE 802.21 [50].

Name	Description
Media Independent Handover Function (MIHF)	The MIHF receives and transmits information about the configuration and condition of access networks around the MN. The MIHF is a logic entity whose definition is independent of its deployment location on the network.
Media Independent Handover Users (MIH Users)	Entities that use the services provided by the MIHF. MIH users use the MIH_SAP to interact with the MIHF. MIH users make handover decisions based on inputs from the MIHF.
Media Independent Command Service (MICS)	The media independent command service (MICS) enables MIH users to manage and control link behaviour relevant to handovers and mobility. Each MIHF shall comprise a MICS.
Media Independent Event Service (MIES)	The media independent event service (MIES) provides event classification, event filtering and event reporting corresponding to dynamic changes in link characteristics, link status, and link quality. Each MIHF shall comprise a MIES.
Media Independent Information Service (MIIS)	The Media Independent Information Service (MIIS) provides the information about different networks and their services thus enabling more effective handover decision to be made across heterogeneous networks. Each MIHF shall comprise a MIIS.
Mobile Node (MN)	A Mobile Node (MN) is defined in as a communication node that can change its point of attachment from one link to another.
Service Access Point (SAP)	The MIHF interfaces with other layers and functional planes using service access points (SAPs). Each SAP consists of a set of service primitives that specify the interactions between the service user and provider.
Point of Attachment (PoA)	The Point of Attachment (PoA) corresponds to the network side endpoint of a layer 2 link that includes a mobile node as the other endpoint.
Point of Service (PoS)	The Point of Service (PoS) can be considered as the MIHF in a Network Entity. MIH Functions communicate with each other for various purposes. The MN exchanges MIH information with its MIH point of service (PoS). The MIHF in any Network Entity becomes an MIH PoS when it communicates directly with an MN-based MIHF.

5.2.1 MIH architecture

Figure 20 depicts an example architecture of MIH with two networks, Wi-Fi and LTE. The interfaces between the devices are also shown (in [50] more interfaces are specified but they does not apply for the scenario presented). In the scenario presented the Mobile Node (MN) has at least two physical interfaces, one LTE interface and a Wi-Fi interface. A more detailed description can be found in Figure 27 below and on section 5.3.

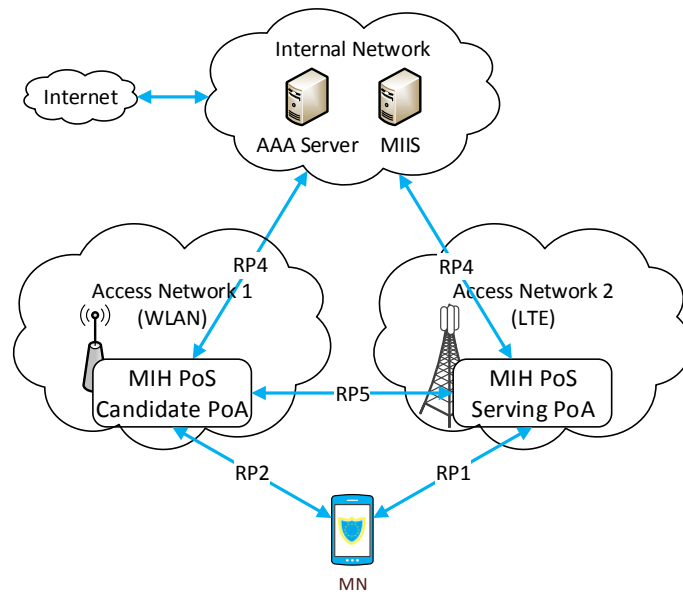


Figure 20 – MIH architecture with LTE and WLAN networks.

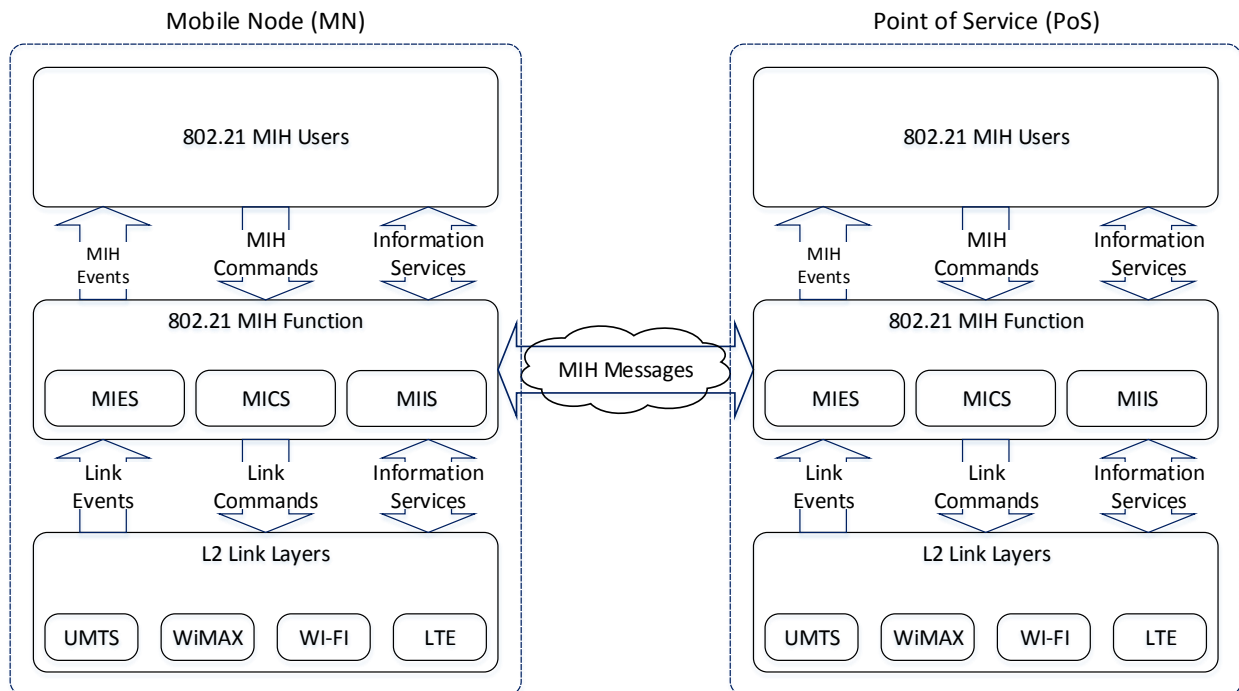


Figure 21 – MIH Architecture in a MN with several physical interfaces.

Figure 21 shows the interaction between the modules and the services associated with MIHF, MICS, MIES and MIIS (see also Table 8). Figure 22 details the relations and connections between the modules of the networks, which are already shown in Figure 20.

Note: the red and green arrows can also be considered as MIH_NET_SAP but they have a different purpose in order to identify the different transport mechanisms allowed by MIH Protocol. The transport mechanisms are described in section 5.2.3 below.

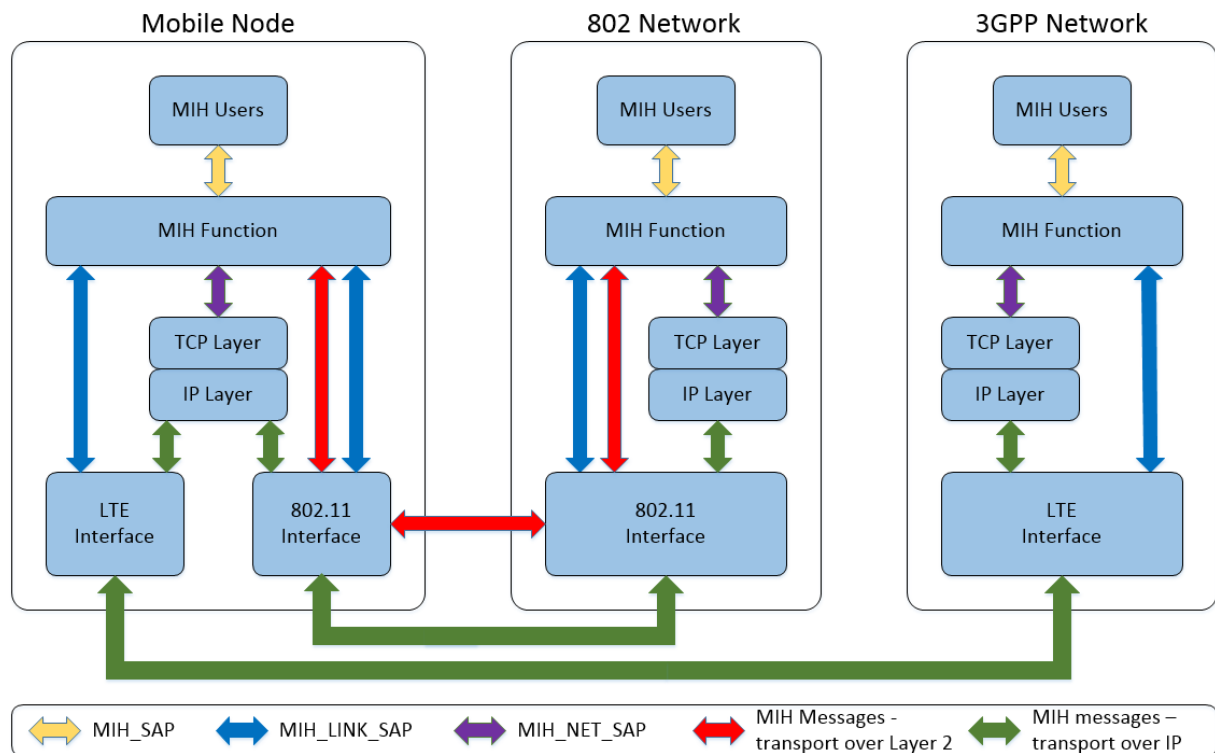


Figure 22 – Types of MIHF relationship (based on [50]).

The general MIH reference model includes the following SAPs:

- MIH_SAP: Media independent interface of MIHF with the upper layers of the protocol stack.
- MIH_LINK_SAP: Abstract media dependent interface of MIHF with the lower layers of the media specific protocol stacks.
- MIH_NET_SAP: Abstract media dependent interface of MIHF that provides transport services over the data plane on the local node, supporting the exchange of MIH information and messages with the remote MIHF. For all transport services over L2, the MIH_NET_SAP uses the primitives specified by the MIH_LINK_SAP.

5.2.2 MIH Protocol Frame

The MIH Protocol Frame structure used to transport MIH messages between remote MIHF are shown in Figure 23 below.

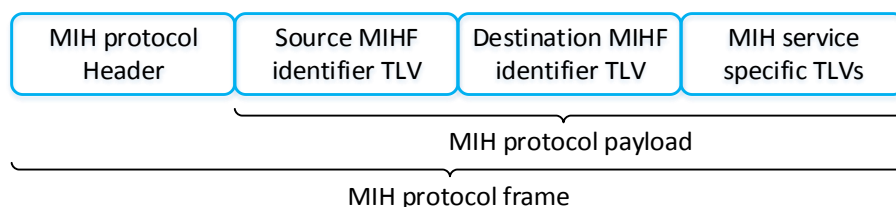


Figure 23 – MIH Protocol Frame [50].

The MIH Protocol Frame is constituted by the following fields:

- MIH protocol header – the header of the MIH message, detailed on section 5.2.2.1;
- Source MIHF identifier TLV – constituted by the MIH identification value (MIHF_ID) of the source;

- Destination MIHF identifier TLV – constituted by the MIH identification value (MIHF_ID) of the destination;
- MIH service specific TLVs – the Information Elements are represented and encoded in Type-Length-Values format and are transported in this field (see [50] for detailed information on TLV format or Information Elements).

5.2.2.1 MIH protocol header format

The MIH protocol header (see Figure 24) carries the essential information that is present in every frame and is used for parsing and analysing the MIH protocol frame.

Note: the MIH Protocol Header format presented in Figure 24 and described in Table 9 complies with the MIH Header format proposed in standard IEEE 802.21a [51] and not with the one proposed in standard IEEE 802.21 [50]. There exist some minor changes between the two versions mainly to support security features. Table 9 describes the fields that compose the MIH Protocol Header.

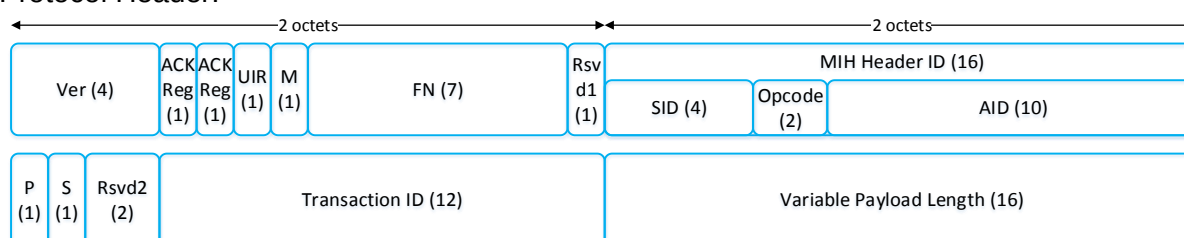


Figure 24 – MIH Protocol Header format.

Table 9 – Description on MIH Protocol Header fields (based on [50] and [51]).

Field name	Size (bits)	Description
Version	4	Identifies the version of MIH protocol used: ▪ 0: Not to be used; ▪ 1: First version; ▪ 2-15: (Reserved)
ACK-Reg	1	This field is used for requesting an acknowledgement for the message (when bit is set to '1')
ACK-Reg	1	This field is used for responding to the request for an acknowledgment for the message (when bit is set to '1')
Unauthenticated information request (UIR)	1	This field is used by the MIH Information Service to indicate if the protocol message is sent in pre-authentication/pre-association state so that the length of the response message can be limited.
More fragment (MF)	1	This field is used for indicating that the message is a fragment to be followed by another fragment.
Fragment number (FN)	7	This field is used for representing the sequence number of a fragment. The fragment number starts from 0. The maximum fragment number is 127.

Reserved 1 (Rsvd1)	1	This field is intentionally kept reserved. When not used, this bit is set to '0'.
MIH Header ID - SID (Service Identifier) - Opcode (Operation code) - AID (Action identifier)	16 4 2 10	The MIH Message ID is combination of SID, Opcode and AID: Identifies the different MIH services, possible values are as follows: - Service Management - Event Service - Command Service - Information Service Type of operation to be performed with respect to the SID, possible values are as follows: - Request - Response - Indication This indicates the action to be taken with regard to the SID (see Table L.1 in 802.21 [50] for AID assignments).
Proactive authentication (P)	1	One bit field that indicates (when set) that the message is a proactive authentication message.
Security association (S)	1	One bit field used for indicate (when set) that a security association exists and the message is protected.
Reserved 2 (Rsvd2)	2	This field is intentionally kept reserved. When not used, all the bits of this field are to be set to '0'.
Transaction ID	12	This field is used for matching Request and Response, as well as matching Request, Response and Indication to an ACK.
Variable payload length	16	Indicates the total length of the variable payload embedded in this MIH protocol frame. The length of the MIH protocol header is NOT included.

5.2.3 MIH Transport mechanisms

MIH messages can be sent over the data plane at both layer 2 and layer 3. If the MIH messages are exchanged in the same network and if layer 2 is an Ethernet based technology then the messages can be sent directly over layer 2 protocol as depicted in Figure 25 below.

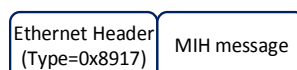


Figure 25 – MIH message encapsulated in an Ethernet frame.

Figure 25 shows the encapsulation of a MIH message in an Ethernet frame. The EtherType value for MIH protocol is 0x8917 (in hexadecimal notation) The MIH protocol guarantees the delivery of the message. Table 9 shows specific fields in the MMIH protocol header for this guarantee.

If the MIH nodes are in different networks or are not directly connected at layer 2 then the transport over layer 3 shall be used. When using transport over layer 3 a transport mechanism shall be used. The transport mechanisms at layer 4 defined in [50] for the transport of MIH messages are the transmission control protocol (TCP), the user datagram protocol (UDP) and the stream control transmission protocol (SCTP). Figure 26 shows an example of a TCP segment carrying a MIH message over layer 4.

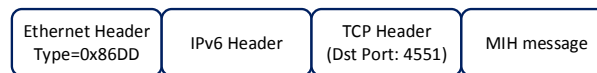


Figure 26 – MIH message encapsulated in an IPv6 packet, using TCP as the transport provider.

5.2.4 MIH security considerations

IEEE 802.21 provides no security features to protect the MIH messages. These have been added on a recent amendment to this standard, IEEE 802.21a [51]. These security features are also described in Deliverable D5.2 [6] which also explains how to integrate them in SALUS.

5.2.5 QoS in MIH

The quality of the service (QoS) experienced by an application depends on the accuracy, speed, and availability of the information transfer in the communication channel. IEEE 802.21 provides support for fulfilling application QoS requirements during handover. In MIH there are two aspects of QoS to consider:

- The QoS experienced by an application during a handover;
- The QoS considered as part of a handover decision.

In section 5.1.4 of [50] is referred that the MIH standard includes mechanisms that support both aspects of QoS towards enabling seamless mobility; however the MIHF alone cannot guarantee seamless mobility. Depending on the QoS requirements of the end-to-end application, seamless mobility implies minimizing the handover latency and packet loss so as to minimize the end-to-end delay and the loss of transmitted information. Seamless mobility also implies the timely assessment of network conditions, such as the monitoring of packet loss on the current link and signal strength from both current and target networks, in order to optimize the handover decision and its execution.

The MIH standard specifies a QoS model that defines parameters that are used to set the requirements and assess the performance of packet transfers between a source and its destinations. When used in threshold-setting commands (such as *MIH_Link_Configure_Thresholds*), these parameters describe the QoS requirements of the MIH user. On the other hand, when used in parameter-reporting events (such as *MIH_Link_Parameters_Report*) and parameter-extraction commands (such as *MIH_Link_Get_Parameters*), they characterize current network conditions. Therefore, depending on their usage these parameters can represent either static QoS requirements or dynamic network measurements.

5.3 Seamless mobility between LTE and other networks

The modules of the Mobility component integrated into the standardized LTE/EPC architecture are shown in Figure 27 in white color. The Mobility component consists of three modules, the Media Aware Proxy module (MAP) for video stream adaptation, the Media Independent

Handover module (MIH) for system monitoring and handover management, and the Proxy Mobile IP module (PMIP) for IP mobility and session continuity.

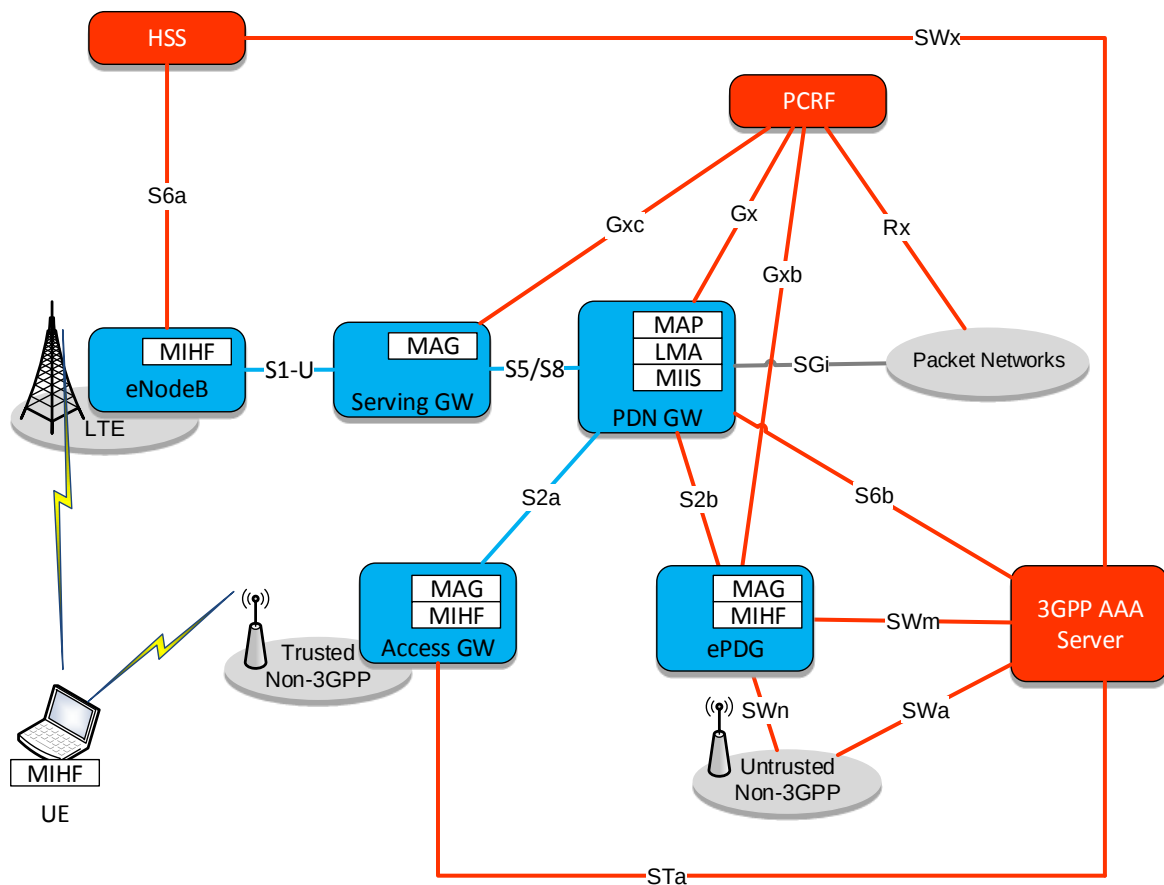


Figure 27 – Mobility modules integrated into the standardized LTE/EPC architecture

SALUS supports full IP Mobility to mobile users through the Evolved Packet Core (EPC) which is the core network of Long Term Evolution (LTE) technology. The protocol that provides IP connectivity using non-3GPP accesses is the Proxy Mobile IP (PMIP) [23][57]. PMIP has been accepted by 3GPP as a supported standard described in [30] and in [31]. The involved entities in the PMIP domain are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). LMA is the home agent for the mobile node and the topological anchor point for the mobile node's home network IP address. MAG is a function on an access router that manages the mobility-related signalling for a mobile node that is attached to its access link. It is responsible for tracking the mobile node's movements to and from the access link and for signalling the mobile node's LMA. A bi-directional tunnel is established between the serving MAG and the LMA, delivering MN's traffic while roaming. According to 3GPP technical specification, the LMA functionality is co-located with the Packet Data Network Gateway (PDN-GW). The MAG functionalities are implemented at the access routers (i.e. Serving-GW, ePDG and Access-GW). The aforementioned architecture fully complies with the standardized one as defined in [30].

Moreover SALUS extends PMIP to support multi-homing in a similar manner to [23], which is an Active-Internet draft of the Network-Based Mobility Extensions Working Group of IETF. As a result, a SALUS client is not only mobile with the ability to roam in a heterogeneous environment but also capable of receiving simultaneously from multiple interfaces.

Additionally, in order to provide link-layer intelligence and other related network information as well as to optimize horizontal and vertical handovers SALUS exploits the Media Independent Handover (MIH 802.21) protocol [28]. A set of handover-enabling functions called MIH Function (MIHF) is used for that purpose. MIHF detects changes in link-layer properties and implements a set of commands that are relevant to handover and switch between links. The other component is the media independent information service (MIIS) that provides details on the characteristics and services provided by the MIHF from both the mobile node and the network side. The information enables efficient system access and effective handover decisions. The MIIS is also located at PDN GW as this node lies at the heart of the EPC, connecting all other entities. The coupling of PMIP with MIH results to a robust mobility management that it guarantees not only reliable handover management but efficient network detection and selection.

Finally, the Media Aware Proxy (MAP) operates as a transparent user-space module used for low delay filtering of scalable multiple description video streams. Its functionality extends from the Network Layer to the Application Layer providing video stream adaptation by taking into account the clients wireless network conditions. MAP receives packets destined to mobile clients and parses their header in order to identify the information without changing the header's fields. Therefore, MAP is able to either drop or forward packets that carry specific layers of a stream to the receiving users. The need for such a middle box stems from the fact that in a real environment each client must be able to have a guaranteed QoE. The MAP function is integrated with PDN-GW and communicates internally with the MIIS database, ensuring fast transmission rate adaptation decisions, whenever required. It is noted that as PDN GW already implements packet lawful interception and routing it can easily adopt the MAP functionalities. Subsequently, MAP inherits the EPC scalability and enhances existing processes to guarantee a minimum QoE level. It is worth noting that in the SALUS implementation the whole process is running at kernel level; hence it is very quick and contributes very little to the overall end-to-end delay.

In MIH two distinct handover decisions are defined within the SALUS platform. The first is called Hard Handover Decision and it is initiated due to signal strength deterioration with only one candidate network, resulting to a horizontal handover. The second is the Quality of Experience (QoE) driven handover decision which is based on upper layer information, hence is an extension to the standard IEEE 802.21 framework and will ensure high QoE to the mobile user.

Below, the signal flows of the horizontal and vertical handover processes are given in Figure 28 and Figure 29 respectively.

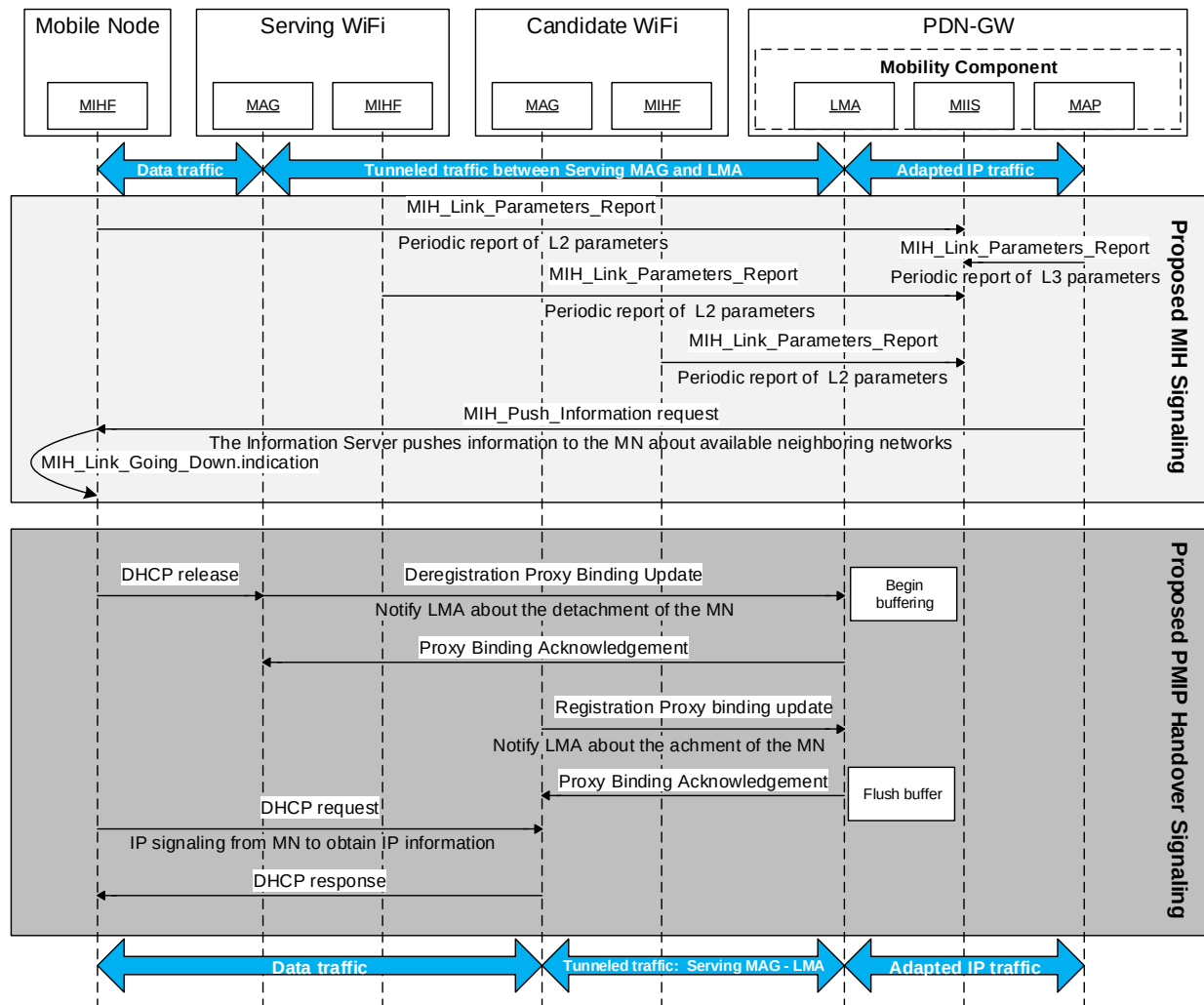


Figure 28 – Horizontal Handover Signalling Flow

Summarized description of the events:

1. The mobile node and the serving and candidate WLAN Access Points (AP) periodically update the MIIS Server of MIH events (changes to monitored metrics) via MIH events service messages called *MIH_Link_Parameters_Report*.
2. Based on the updated information on the network and user side metrics, the MIH Server pushes information regarding availability and priority of neighbouring networks to the MN using the *MIH_Push_Information* message.
3. The MIH event *MIH_Link_Going_Down* indicates to the MN that a handover is imminent. As a result the MN sends a DHCP release message to the current MAG, which in turn deregisters the MN from the LMA using a Proxy Binding Update (PBU) message. Upon receiving the deregistration PBU message the LMA starts buffering packets destined to the MN.
4. Afterwards the MN establishes a link connection with the new AP. The MAG detects the new attachment and informs the LMA for the MN's new location. The LMA registers the MN and forward the buffered packets to the MN through the new MAG.
5. Finally, a DHCP handshake takes place orchestrated by the MAG, that allows the MN to continue using the same IP address at the new AP and by that enabling IP mobility and session continuity.

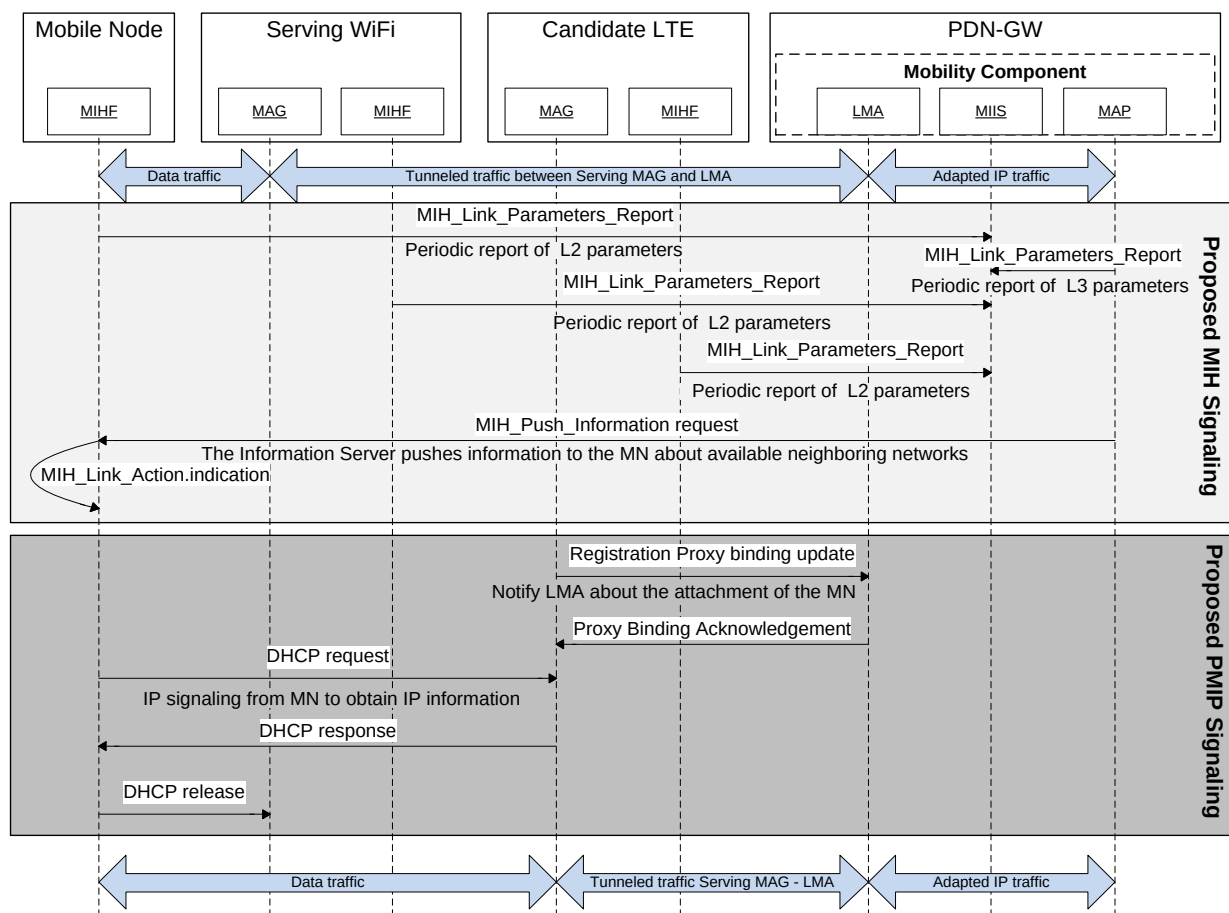


Figure 29 – Vertical Handover Signalling Flow

Summarized description of the events:

1. As in the previous scenario the MN, the serving and candidate WLAN AP periodically update the MIIS Server with MIH_Link_Parameters_Report messages while MIIS Server responds with the MIH_Push_Information message.
2. However in this scenario the received policy list indicates a vertical handover and triggers a link switch at the mobile node. The MIH_Link_Action primitive is utilized to generate a change of the active interface at the MN.
3. Once the MN establishes a link connection with the new access network, the MAG detects the new attachment and informs the LMA for the MN's new location. The LMA registers the MN and forwards the MN's traffic through the new MAG.
4. Finally, a DHCP handshake takes place orchestrated by the MAG, that allows the MN to continue using the same IP address at the new point of attachment. It is noted that, as the previous interface is detached only after the new has established its IP connectivity no buffering is needed due to a "make-before-break" handover process.

The multi-homing scenario signalling flow is the same with vertical handover with the exception of no link detachment for the current interface. Additionally, an enhanced PBU is used to inform the LMA that the MN must obtain the same IP address as already assigned to the existing session without removing this session, as described in [23]. The LMA uses enhanced functionalities to support load balancing between the two simultaneously active interfaces.

5.4 QoS and PMIP for 802.11

Within the context of SALUS we are considering next generation wireless systems that are based on LTE. In LTE Core network (Enhanced Packet Core), mobility is handled by PMIP. The PPDR Communication Systems can require Vertical or Horizontal Handover between different communication technologies such as LTE and Wi-Fi. One of the challenges is to maintain QoS when the MT hands off over Wi-Fi. This is describes in this subsection.

The TSPEC element in 802.11 contains the set of parameters that define the characteristics and QoS expectations of a traffic flow. TSPEC in IEEE 802.11 is used to reserve QoS for a traffic stream (MN MAC, TS (Traffic Stream) id). [32] QoS reservation is used for IEEE 802.11 protocols that are associated with a Mobile Node's MAC address. The PMIPv6 QoS flow is identified by the TCLAS element. The TCLAS element specifies an element that contains a set of parameters necessary to identify incoming MSDU (MAC Service Data Unit) that belong to a particular TS (Traffic Stream) [33]. When TCLAS is present, a one-to-one mapping between the TCLAS defined flow and the Traffic Selector is given as shown in Table 10 [32].

Table 10 – IEEE 802.11 and PMIPv6 QoS Connection mapping

MN <--> AP(IEEE 802.11)	MAG <--> LMA (PMIPv6)
(TCLAS Classifier 1)TCP/UDP IP (TCLAS Classifier 1) DSCP	Traffic Selector (IP flow) Traffic Class (TC)

The QoS reservation request in 802.11 is derived as presented in Table 11 when the MN or AP is not able to convey flow parameters in TCLAS.

Table 11 – WMM and PMIPv6 QoS Connection mapping

MN <--> AP (WMM)	MAG <--> LMA (PMIPv6)
no IP flow parameter/TCLAS	(a) applies to all flows (b) derived out-of-band
User Priority (802.1D)	Traffic Class (TC)

When mapping between Access Class is used and TCLAS is not present to specify IP flow, one of two options apply for the MAG - LMA (PMIPv6) segment:

1. Bandwidth parameters apply to all flows of the MN. This is not a preferred mode of operation if the LMA performs reservation for a single flow, e.g. a voice flow identified by an IP 5-tuple.
2. The IP flow for which the MN requests reservation is derived out-of-band. For instance the AP/MAG observes application level signalling (e.g. SIP) or session level signalling (e.g. 3GPP WCS [34]) and associates subsequent ADDTS request using heuristics and then derives the IP flow/Traffic Selector field [32].

Table 12 contains a mapping between Access Class (WMM AC) and 802.1D in IEEE 802.11 frames and DSCP in IP data packets. The table also shows the mapping between Access Class (WMM AC) and DSCP for use in IEEE 802.11 TSPEC and PMIPv6 QoS (Traffic Class).

Table 12 – QoS Mapping between QCI/DSCP, 802.1D UP, WMM AC

QCI	DSCP	802.1D UP	WMM AC	Example Services
1	EF	6(VO)	3 AC_VO	conversational voice
2	EF	6(VO)	3 AC_VO	conversational video
3	EF	6(VO)	3 AC_VO	real-time gaming
4	AF41	5(VI)	2 AC_VI	buffered streaming
5	AF31	4(CL)	2 AC_VI	signaling
6	AF32	4(CL)	2 AC_VI	buffered streaming
7	AF21	3(EF)	0 AC_BE	interactive gaming
8	AF11	1(BE)	0 AC_BE	web access
9	BE	0(BK)	1 AC_BK	e-mail

The MN tags all data packets with DSCP and 802.1D UP equivalent to the application and the subscribed policy or authorization. The AP polices sessions and flows based on the configured QoS policy values for the MN [32].

For QoS reservations, TSPEC uses WMM AC values and PMIPv6 QoS uses corresponding DSCP values in Traffic Class (TC). IEEE 802.11 QoS Access Class AC_VO, AC_VI are used for QoS reservations. AC_BE, AC_BK should not be used in reservations. When WMM-AC specifications that do not contain TCLAS are used, it is only probable to contain one reservation per Traffic Class / access category (AC). PMIPv6 QoS will not contain any flow specific attributes like Traffic Selector.

Bandwidth parameters that need to be mapped between IEEE 802.11 and PMIP QoS are shown in Table 13.

Table 13 – Admission Controlled Flows - Bandwidth Parameters

MN <--> AP(IEEE 802.11)	MAG <--> LMA (PMIPv6)
Mean Data Rate, DL	Guaranteed-DL-Bit-Rate
Mean Data Rate, UL	Guaranteed-UL-Bit-Rate
Peak Data Rate, DL	Aggregate-Max-DL-Bit-Rate
Peak Data Rate, UL	Aggregate-Max-UL-Bit-Rate

PMIPv6 QoS guarantees that congestion related packet drops will not happen, when using the Guaranteed Bit Rate (GBR). IEEE 802.11 radio networks provide no such guarantee. The TSPEC be supposed to include Mean Data Rate and it is recommended that it be mapped to the GBR parameters, Guaranteed-DL-Bit-Rate and Guaranteed-UL-Bit-Rate in PMIPv6 QoS [35].

IEEE 802.11 TSPEC do not require fields, like Peak Data Rate to be completed, however for MNs and APs that are capable of specifying the Peak Data Rate, it should be mapped to MBR (Maximum Bit Rate) in PMIPv6 QoS. The AP ought to use the MBR parameters, Aggregate-

Max-DL-Bit-Rate and Aggregate-Max-UL-Bit-Rate to police these flows on the backhaul segment between MAG and LMA.

5.5 Multicasting in mobile networks

Real time services are delivered as multimedia streaming, which means that they require higher network resources, especially when delivered to each user separately. Multicast delivery will reduce the huge demands of bandwidth for such services. Additionally, hardware load on media servers is reduced when using multicast. Furthermore, routers only need to manage a single data stream.

Multicast connection management is performed by multicast agents in WLAN and cellular heterogeneous networks. MNs can make handoff decisions to activate the proper network interface switching to avoid discontinuities in the delivery of multimedia application services. The most important handoff metrics are the network-related parameters used for making the decision such as bandwidth, load, latency and traffic congestion that are useful for load balancing across different type of networks and QoS. An additional consideration in multicast connection management is the type of application, as different types of applications require different QoS parameters. This includes the data rates and the reliability of networks the multimedia applications require. Finally, other important handoff metrics are the connection cost between users and network operators and the battery power of MNs.

5.5.1 Multicast mobility problems and multicast mobility support

When trying to deliver a multicast packet to mobile nodes, a number of factors need to be considered, such as the location of the nodes. If a node located in a region covered by its Home Agent (HA) moves to an area covered by a different agent, then duplicate multicast packages are transmitted over more than one tunnel. To solve this problem, Jeon et al. [41] proposed a multicast network model using PMIPv6. They separate the MR function from the LMA, so that the MAG can connect to both the LMA and the MR. Thus, multicast packets are delivered from the MR while unicast packets are delivered from the LMA via tunnels. However, the overhead from the routing update reduces the performance of PMIPv6 components.

There are two possible methods of multicast mobility support that should be considered:

- **Using a tunnel between the previous MAR (A-MAR) and the serving MAR (S-MAR):** This method follows the unicast mobility solution as proposed in [30], and the multicast traffic is directed through the mobility tunnel. This behaviour is like the behaviour of PMIPv6: the A-MAR, where the flow was initially created, is the Local Mobility Anchor (LMA) while the S-MAR is equivalent to the Mobile Access Gateway (MAG). However, the existence of the tunnel creates some questions as to the packet and processing overhead, and non-optimal routing. Moreover, when multicast listener mobility is considered, the tunnel convergence problem needs to be taken into account, especially in high mobility environments [40].
- **Using the multicast infrastructure for sending/receiving the traffic. Besides, a MAR can act as a MLD Proxy or multicast router (MR):** This second method takes advantage of the native multicast infrastructure for delivering multicast traffic, hence avoiding the tunnelling overhead.

5.5.2 Multicast Source and Listener Mobility

As mentioned before, the considered method for source mobility support follows the unicast mobility solution. When mobility occurs, the multicast traffic is directed through the mobility tunnel from the S-MAR to the A-MAR, and then to the multicast tree, ending to the listeners using multicast routing protocols. As a result, the activation of Shortest Path Tree (SPT) does not provide any advantages since the traffic would follow a similar route to the listeners, and pass by the AMAR.

Furthermore, it would increase the signalling overhead which is proportional to the amount of listener's Designated Routers (DR) and to the number of PIM Joins/Prunes [28]. From source multicast point of view, it is the easiest way to deploy and more advantageous in mobile scenarios. Namely, the A-MAR may be set as the RP of the session, making sure the tunnel endpoint is simultaneously the RP. As such, the stability of multicast delivery tree is guaranteed. Besides, no extension is required for the Protocol Independent Multicast Sparse Mode (PIM-SM [28]) protocol.

5.5.3 Multicast Listener Mobility

Using the second method, the S-MAR simply sends, on behalf of the MN, join messages to the neighbour DRs. Thus, the multicast traffic is directed from the native multicast infrastructure to the S-MAR, and the mobility tunnel configured for unicast is not used for multicast operations. When moving between MARs, a multicast listener demonstrates a certain delay in receiving multicast content, because of the extra time related to the MLD Report transmission, and possible PIM signalling by S-MAR, compared to unicast sessions. [25] This means that the strict requirements of real-time applications may not be fulfilled. Having that in mind, a solution incorporating multicast context transfer is needed in order to solve this problem. [37] Thus, Context Transfer is proposed for exchanging multicast-related information between two MARs. Upon receiving the request from its Flow Manager (FM), the S-MAR triggers a Context Transfer request towards the A-MAR to request the MN's active multicast subscription information. The receiving MAR will check multicast subscription information regarding the corresponding MN, based on multicast group management protocols. It then replies to the S-MAR with a Context Transfer response message which corresponds to the MN's multicast-related information. Upon receiving the multicast subscription information, the S-MAR joins the necessary multicast trees. From that instant, the multicast content is ready to be sent to the MN.

5.5.4 Base solution for mobile multicast source support in PMIPv6 networks

This section describes how Multicast can be applied to SALUS and PPDR Communication Systems. In Public Safety, the headquarters/NOC may send real time messaging and/or video to several PPDR users concurrently. Some of these users may be in fixed locations (e.g. fire brigade local station) while some other are on the move (e.g. emergency vehicles). This scenario can be supported using IP Multicasting.

In the Base Solution (BS) for multicast source mobility, just as in the BS for receiver mobility in RFC6224 [19] the Multicast Listener Discovery (MLD) proxy functions are deployed at the MAGs to allocate multicast data in PMIPv6 networks. The MLD proxy instance serving a mobile multicast source (MN) configures its upstream interface at the tunnel towards the MN's corresponding LMA. This base deployment is the simplest way to PMIPv6 multicast extensions meaning that it follows the common PMIPv6 traffic model without the requirements of new protocol operations and additional infrastructure entities. In Figure 30 the reference scenario of the BS for mobile multicast source support in PMIPv6 networks is shown, where the LMAs serve as multicast anchor points and the MAGs are the first-hop access routers serving multiple MNs on the downstream, and run an MLD proxy instance for every LMA upstream tunnel as well. In Figure 30 MN1 and MN3 are mobile multicast sources, whereas the MN2 and all the

correspondent nodes (CNs) are multicast receivers [24]. In this scenario, mobile sources always remain agnostic of multicast mobility operations.

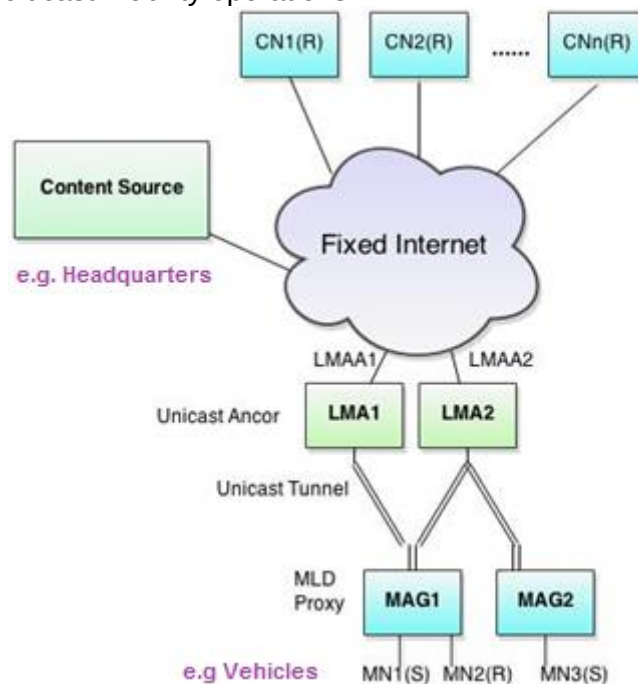


Figure 30 – Mobile multicast source support in PMIPv6 networks

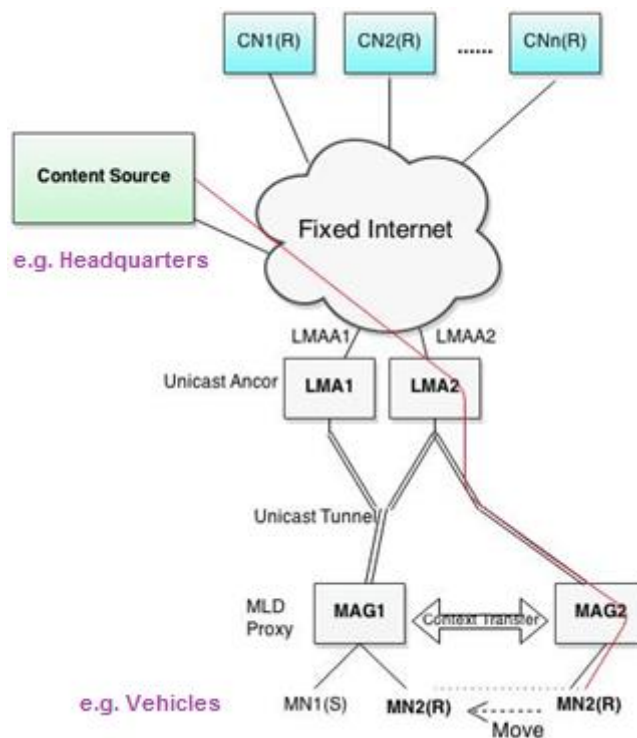


Figure 31 – Mobile multicast source support in PMIPv6 networks - Movement of Mobile Node Receiver (MN2)

As specified in RFC4605 [25] the multicast data originated from the MN1 will arrive at the MAG1 at first, and then arrive at the LMA1 and directly at the MN2 attached to the same MAG with the MN1 via the MLD proxy function at the MAG1. Serving as the Protocol-Independent Multicast

(PIM) designated router (DR), the LMA1 will encapsulate the multicast packets and forward the data to the virtual interface with encapsulation target rendezvous point (RP) (G), which is the SR case. After receiving the SR packets, the RP will decapsulate and forward the packets down the RP-based distribution tree towards the receivers and initiate a source-specific join for creating a SPT to the mobile source MN1(S) and issue a source register stop at the arrival of data from S. Since the LMA1 is the topological anchor point of the mobile source MN1 in the PMIPv6 network, the (S, G) tree will proceed from the RP via the LMA1 and then the LMA1-MAG1 tunnel to the mobile source, which is the SPT case. Because of the excessive packet transmission, the DRs of receivers will initiate a source-specific join for creating a SPT to the mobile source S, thereby the (S, G) tree will proceed from the receiving DR via the LMA1 and then the LMA1-MAG1 tunnel to the mobile source, which is the source-specific multicast (SSM) case.

When the multicast source MN1 moves from the MAG1 to the MAG2, it is able to send multicast packets as soon as network connectivity is reconfigured. At this time, the MAG2 firstly determines whether the MN1 is permissible to multicast services and then performs the binding registration to the LMA1, including the IPv6 unicast address configuration. Besides, the MAG2 adds the new downstream link to the MLD proxy instance with upstream link to the LMA1. Therefore, when the MN1 accesses the MAG2, multicast packets reaching the MAG2 will be forwarded again to the LMA1. Because the LMA1 is always the DR for the mobile multicast source MN1, the multicast data will eventually be forwarded to the receivers by the LMA1 according to the forwarding states maintained by multicast routing. The detailed handover process call flow is shown in Figure 32, in which ‘MLD Membership Report’ is abbreviated by ‘Join.’

As illustrated in Figure 31, when the MN1 attaches to the MAG1, the multicast packets sent by it could be delivered to the CNs through the LMA1 and directly sent to the MN2 attached to the same MAG with the MN1 via the MLD proxy function at the MAG1. When the MN1 hands over to the MAG2, as soon as the binding update to the LMA1 and MLD proxy downstream and upstream interface configuration at the MAG2 has been processed and also the IP address at the MN1 has been configured, the multicast packets can be successfully transmitted by the MAG2 to the LMA1 and then to the corresponding receivers CNs and MN2. In this way, the multicast source mobility is transparently enabled in multicast-deployed PMIPv6 networks. Besides, the LMA can serve as an additional MLD proxy.

These multicast deployment considerations apply to the MNs that operate with their IPv4 stack enabled in PMIPv6 networks. RFC5844 [38] provides that the IPv4 home address mobility support in PMIPv6 networks, and an Internet Group Management Protocol (IGMP) proxy function at the MAG can support IPv4 multicast in an analogous way. However, there exists routing inefficiency problem in this solution. If the mobile receiver MN2 attaches to the same MAG1 as the mobile source MN1 but associates with a different LMA, the multicast traffic has to flow up to the LMA1, cross over to the LMA2, and then be tunnelled downwards to the MAG1, causing redundant, as shown in Figure 32.

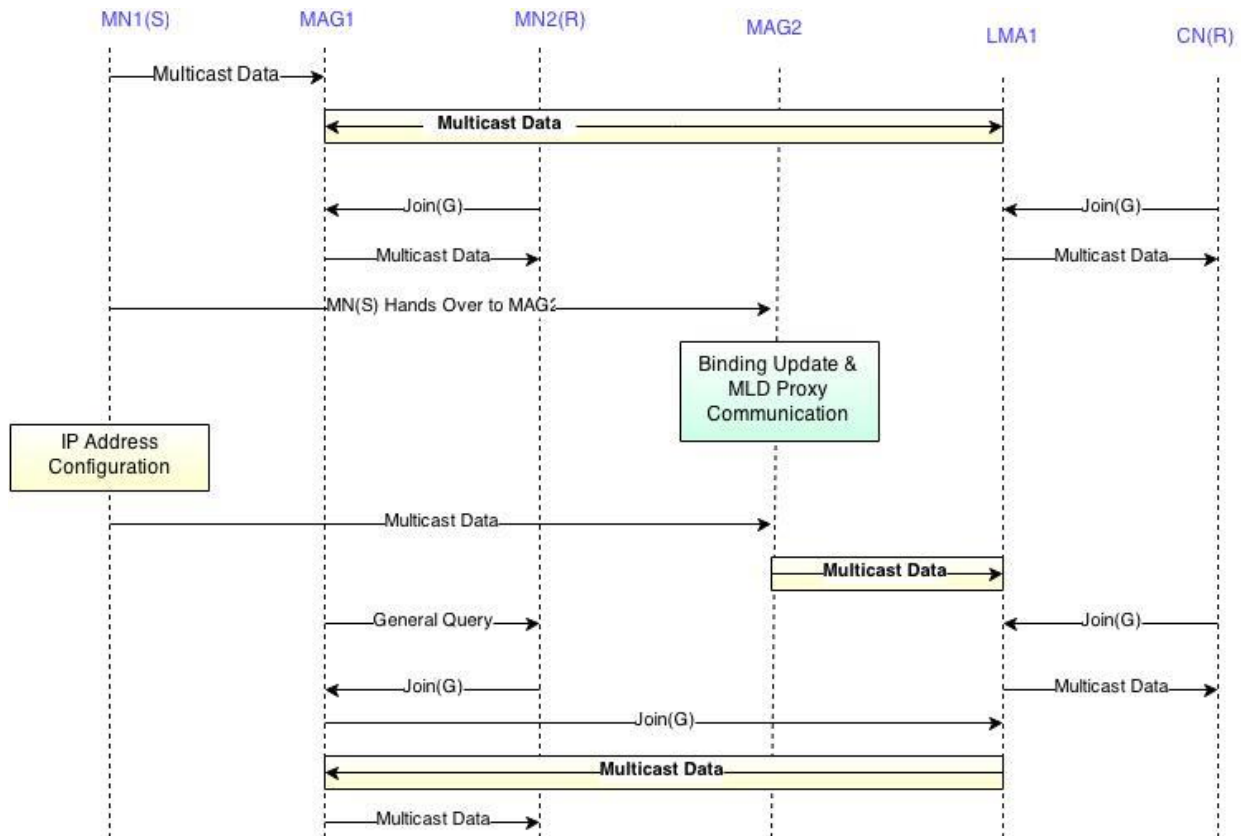


Figure 32 – Group communication in Multicast-deployed PMIPv6 networks

5.5.5 Multicast Challenges and QoS

In terms of research on Logical Interface solutions [25], PMIPv6 scenarios provide inter-technology mobility and multi-homing which require specific software configurations at the mobile node. Packet loss needs to be considered when a mobile node is the traffic source, even though there are no efforts regarding uplink connectivity, or vertical handover issues when a mobile node is moving between MAGs whatsoever. To be more precise, the vertical handover of a source creates the need of synchronization between different layers of handover processes. Moreover, applications that rely on IP multicast, cannot invoke the subscription on the target interface [26].

6 LTE RESILIENCE ASPECTS

This section gives a preliminary view of the LTE resiliency aspects. Figure 33 shows a simplified overview of the LTE architecture.

As already mentioned, LTE is an all-IP system. The system basically allows interconnecting any node with one or more nodes in the architecture hierarchy for both data and signalling. Although this was already possible in the previous cellular operations at core network level, it is now possible with LTE to have each eNB connected to multiple SGW and MME. In nominal situation, this feature is used to load balance the traffic and signalling load but in the event of the failure of a SGW or an MME, the corresponding traffic can be handled by one of the other node connected to the eNB.

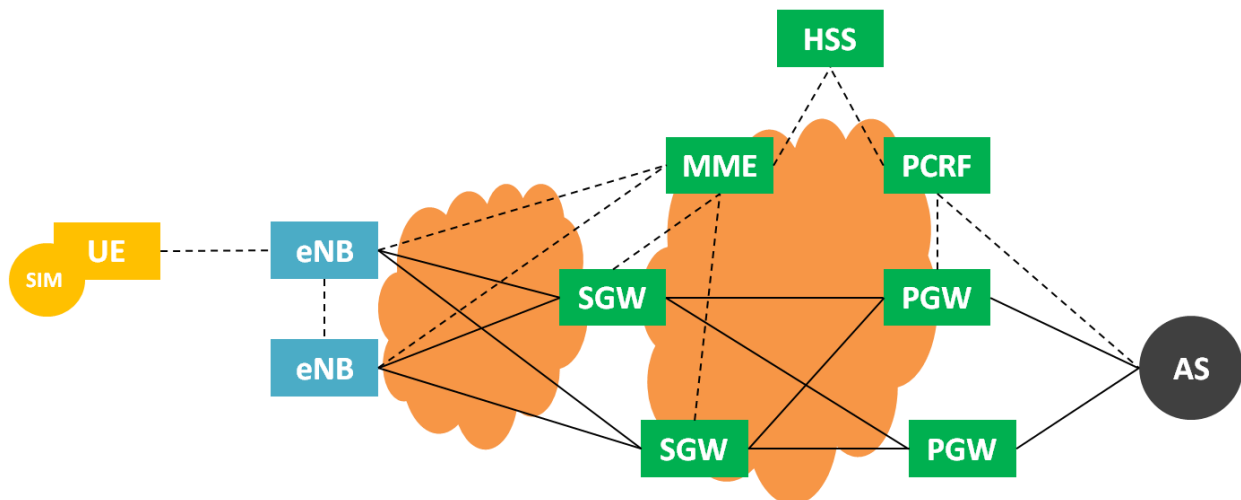


Figure 33 – LTE resilient architecture (simplified)

Also, the system being all-IP, all the nodes are interconnected via a managed packet transport network (e.g. using IP/MPLS). Such transport system can offer transparent restoration of the path provided appropriate design and traffic engineering have been previously performed.

The 3GPP community is planning to further improve the resiliency by mimicking a TETRA feature (call Fallback mode) where the TETRA base station can still provide services in its area even if disconnected from the main switching centres. This feature, called IOPS (Isolated E-UTRAN operations) in 3GPP is currently a study item for the release 13. It is also to be noted that this “Proximity Service” (ProSe), when available will also provide a level of resiliency allowing PPDR users to connect directly in the absence of coverage from the infrastructure.

7 NETWORK MANAGEMENT

7.1 Introduction

Network management is crucial for deployment of the services to the end-users. In particular when providing a mix of services, as is the case for the next generation PPDR services. Network management can be seen as a provisioning layer, on top of the operational system. The management of all PPDR enabled devices, which collectively provide communication services, is very complex. The complexity is aggravated by the number of elements which generate data and by the sheer volume of the data. The SALUS system architecture contains a number of subsystems, in particular TETRA, TETRAPOL, LTE and WLAN systems that need to be monitored/supervised. This section provides an intermediate description of the NMS related to SALUS, focusing on the next generation PPDR technologies.

The definition of network management means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with an outdated protocol analyzer. In other cases, network management involves a distributed database, auto polling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks, providing information such as router traffic, QoS, QoE, intrusion detection, reporting and alerting on network and systems availability, usually under the control of a friendly, web-based GUI.

7.2 Network Management System (NMS)

A Network Management System (NMS) is a set of hardware and software tools that allow supervising the individual components of a network, within a larger network management framework. Network management system components assist with:

- Network Device Discovery – identifying what devices are present on a network.
- Network Device Monitoring – monitoring the devices to determine the health of network components and the extent to which their performance matches capacity plans.
- Network Performance Analysis – tracing performance indicators such as bandwidth utilization, packet loss, latency, availability and uptime of routers, switches and other Simple Network Management Protocol (SNMP) supported devices.
- Intelligent notifications – configurable alerts that will respond to specific network scenarios by paging, emailing, calling or texting a network administrator.

The International Organization for Standardization (ISO) network management model defines five functional areas of network management: Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management (FCAPS).

7.2.1 FCAPS Model

7.2.1.1 Fault Management

The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems, to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

The purpose of fault management is to detect, isolate, notify, and correct faults encountered in the network. Network devices are capable of alerting management stations when a fault occurs on the systems. An effective fault management system consists of several subsystems. Fault detection is accomplished when the devices send SNMP trap messages, SNMP polling, remote monitoring (RMON) thresholds, and syslog messages. A management system alerts the end user when a fault is reported and corrective actions can be taken.

With an increasing number of network elements and complexity of network issues, an event management system that is capable of correlating different network events (syslog, trap, log files) may be considered. This architecture behind an event management system is comparable to a Manager of Managers (MOM) system. A well-designed event management system allows personnel in the Command & Control Centre (CCC) to be proactive and effective in detecting and diagnosing network issues. Event prioritization and suppression allow network operation personnel to focus on critical network events, investigate several event management systems.

7.2.1.2 Configuration Management

The goal of configuration management is to monitor network and system configuration information, so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

With an increasing number of network devices deployed, it is critical to be able to accurately identify the location of a network device. This location information should provide a detailed description meaningful to those tasked with dispatching resources when a network problem occurs. Naming conventions for network devices, starting from device name to individual interface, should be planned and implemented as part of the configuration standard. A well-defined naming convention provides personnel with the ability to provide accurate information when troubleshooting network problems. The naming convention for devices can use geographical location, building name, floor, and so forth. For the interface naming convention, it can include the segment to which a port is connected, name of connecting hub, and so forth. On serial interfaces, it should include actual bandwidth, local data link connection identifier (DLCI) number (if Frame Relay), destination, and the circuit ID or information provided by the carrier.

When a network manager add new configuration commands on existing network devices needs, it's necessary to verify the commands for integrity before the actual implementations takes place. An improperly configured network device can have a disastrous effect on network connectivity and performance. Configuration command parameters must be checked to avoid mismatches or incompatibility issues. The discovery function of most network management platforms is intended to provide a dynamic listing of devices found in the network. Discovery engines such as those implemented in network management platforms should be utilized. The upgrade window to complete device maintenance is fairly limited for some organizations. In a large network environment with limited resources, it might be necessary to schedule and

automate software upgrades after business hours. The procedure can be completed either using scripting language such as expect or an application written specifically to perform such a task.

7.2.1.3 Accounting Management

Accounting management is the process used to measure network utilization parameters, so that individual or group users on the network can be regulated appropriately for the purposes of accounting or chargeback. Similar to performance management, the first step toward appropriate accounting management is to measure the utilization of all important network resources. Network resource utilization can be measured using NetFlow and IP Accounting features. Analysis of the data gathered through these methods provides insight into current usage patterns.

The data can be collected via probes or NetFlow. Shareware applications such as cflowd are also used to gather NetFlow data. An on-going measurement of resource usage can yield billing information, as well as provide information to assess continued fair and optimal resource usage. Understand application-driven data collection requirements. Accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end-to-end view. Understand the impact of network topology and routing policy on flow collection strategy.

By enabling IP accounting, users can see the number of bytes and packets switched through the OS software on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis. Traffic generated by the software or terminating in the software is not included in the accounting statistics. To maintain accurate accounting totals, the software maintains two accounting databases: an active and a check-pointed database.

7.2.1.4 Performance Management

Performance statistics of wide-area network (WAN) technologies, including Frame Relay, ATM, Integrated Services Digital Network (ISDN) and others, can be monitored and collected. Different performance metrics at the interface, device, and protocol levels should be collected on a regular basis using SNMP. The polling engine in a network management system can be utilized for data collection purposes. Most network management systems are capable of collecting, storing, and presenting polled data.

Various interface statistics can be collected from network devices to measure the performance level. Statistics such as input queue drops, output queue drops, and ignored packets are useful for diagnosing performance-related problems. At the device level, performance metrics can include CPU utilization, buffer allocation (big buffer, medium buffer, misses, hit ratio), and memory allocation. The performance of certain network protocols is directly related to buffer availability in network devices. Measuring device-level performance statistics are critical in optimizing the performance of higher-level protocols.

User traffic has increased significantly and has placed a higher demand on network resources. Network managers typically have a limited view on the types of traffic running in the network. User and application traffic profiling provides a detailed view of the traffic in the network. Two technologies, RMON probes and NetFlow, provide the ability to collect traffic profiles. Various solutions are available in the marketplace to address the needs of performance management for enterprise environments. These systems are capable of collecting, storing, and presenting

data from network devices and servers. The web-based interface on most products makes the performance data accessible from anywhere in the enterprise.

7.2.1.5 Security Management

The goal of security management is to control access to network resources according to local guidelines, so that the network cannot be sabotaged (intentionally or unintentionally). A security management subsystem, for example, can monitor users logging on to a network resource, refusing access to those who enter inappropriate access codes. Security management is a very broad subject; therefore this area only covers security as related to SNMP and basic device access security.

Detailed information on advanced security includes Increasing Security on IP Networks and Open Systems. A good security management implementation starts with sound security policies and procedures in place. It is important to create a platform-specific minimum configuration standard for all routers and switches that follow industry best practices for security and performance. There are various methods of controlling access on routers and catalyst switches. Some of these methods include Access Control Lists (ACL), User IDs and passwords local to the device and Terminal Access Controller Access Control System (TACACS).

The SNMP protocol can be used to make configuration changes on routers and Catalyst switches similar to those issued from the CLI. Proper security measures should be configured on network devices to prevent unauthorized access and change via SNMP. Community strings should follow the standard password guidelines for length, characters, and difficulty of guessing. It is important to change the community strings from their public and private defaults. All SNMP management host(s) should have a static IP address and be explicitly granted SNMP communication rights with the network device by that predefined by IP address and Access Control List (ACL).

Authentication is the process of identifying users, including login and password dialog, challenge and response, and messaging support. Authentication is the way a user is identified prior to being allowed access to the router or switch. There is a fundamental relationship between authentication and authorization. The more authorization privileges a user receives, the stronger the authentication should be. Accounting allows for the collecting and sending of security information used for billing, auditing, and reporting, such as user identities, start and stop times, and executed commands. Accounting enables network managers to track the services that users are accessing as well as the amount of network resources they are consuming.

7.2.2 Network Management Architecture

The information on this subsection has been considered security sensitive and it has been moved to D6.1 RESTREINT EU Annex, which is a separated document (SALUS_D6.1_Annex_v1.0.docx)

7.3 LTE Network Management System

A major challenge for PPDR organizations is to ensure their readiness to act, anytime, anywhere. Meeting this challenge heavily depends on availability of emergency communications (that will combine in the future mode of operations several radio access networks including LTE) in the response area. To manage and operate the network efficiently, PPDR network operators

will require an advanced Network Management System that will provide easy configuration of the complex sub-systems, efficient monitoring and supervision of the network and services availability and fast troubleshooting in case of a failure.

LTE will bring new capabilities to PPDR users based on a new broadband IP based technology. This will add an additional layer of complexity to the network management tasks. Besides, contrary to legacy circuit switched based systems, the management of the LTE system must take into account the services that cross the LTE network and not only the elements of the system. Indeed, in a circuit switched system, the failure of a circuit causes the loss of the service using this circuit. In packet based (IP) systems, services might be affected by several events (failure of a link, congestion...) which may cause a degradation of a service and not necessarily a complete loss of the service.

Consequently, an efficient LTE NMS should provide a service-aware end-to-end management (for data and control plane) with a unified view on all the network domains (LTE Radio Access Network, packet based backhaul and LTE packet core). This multi-layer E2E view must span the different features of the LTE NMS:

- Automated configuration and flexible tools to minimize operator error and decrease downtime durations. Based on rules and inputs from other tools (e.g. radio network planning and optimization tools) this allows to perform bulk provisioning for large (evolving) networks. The same tool can also run configuration policy audits that verify deployed configurations in the network to identify discrepancies and help the network operator correct or not the discrepancies (note, some discrepancies might actually be specific configurations for a specific set of nodes).
- Proactive assurance capabilities across the different layers to simplify management tasks of supervision. The NMS should provide intelligent alarm creation based on events generated by network elements, and alarm correlation from alarms and events from different layers to allow an operator to quickly understand the root cause and to resolve it. This type of information can also be compared to predefined SLAs (connectivity, delay, jitter...) and can raise an alarm or an event in case a SLA performance indicator is violated. The same can be used as well to collect information on key performance statistics.

LTE NMS should also have an open architecture (e.g. based on 3GPP and XML Northbound interfaces) to ease its integration with other operational processes and systems such as an Operations Support System (OSS) that would have a complete network operation and support view on all the sub-systems of a future PPDR system (e.g. including the TETRA and/or TETRAPOL sub-systems, Wi-Fi...).

Beyond the traditional NMS approach, 3GPP has defined standard advanced features, SON (Self-configuring and self-optimizing network), that help LTE network operators to better and more easily configure and optimize the LTE access network by automatizing some of the network operation processes [48], [49].

SON features can be divided into three main categories:

- Self-configuration – this corresponds to automatic setting of simple eNB parameters such as Physical Cell Identity (PCI), transmission power, Automatic Neighbour Relations (ANR); this will allow the network operator and planner to save time during the provisioning phase and will allow them to concentrate on other more important tasks.

- Self-optimisation – this may include optimisation of coverage, capacity, handovers and interference. This feature avoids lengthy measurement campaigns and optimisation exercise to improve the network performances and can be fully autonomous or controlled by the network operator.
- Self-healing – this provides automatic detection and removal of failures through automatic adjustment of parameters. For instance, in case of a failure of a cell, the surrounding cells may increase their transmission power to mitigate (part of) the coverage hole left by the cell in failure and change the ANR list accordingly.

SON requires the collaboration of UEs to operate since it is based on continuous information / reports coming from UEs that are actually in the coverage area. It is expected that SON will be beneficial to PPDR users to ensure the best performance of the network without having to perform extensive and costly specialized drive testing on a permanent infrastructure. Also, deployment a (set of) eNB to provide more capacity / coverage in an area where a major event occurs will be simplified.

7.4 WLAN ad-hoc Network Management System

The information on this subsection has been considered security sensitive and it has been moved to D6.1 RESTREINT EU Annex, which is a separated document (SALUS_D6.1_Annex_v1.0.docx)

8 CONCLUSIONS

This document contains the intermediate description of the SALUS research into connectivity, QoS provisioning and seamless mobility in heterogeneous networks. This intermediate description focuses on current solutions and principles, applied to the foreseen PPDR system. Mission critical communication for PPDR services implies that services are offered with at least a certain minimum quality level, and that the services can be used while mobile in complex situations. These requirements imply that QoS and seamless mobility are two of the most key features of PPDR communication services.

The foreseen broadband PPDR system is to carry a large variety of services over a number of radio technologies. The variety of services translates into a set of QoS parameters that are mapped to the LTE/SAE structure of the QCI, the QoS Class Indicator. Using this LTE/SAE based structure is shown to provide sufficient modularity to cater for the variety of PPDR services that were identified in WP2. The QoS toolset of LTE/SAE is expected to provide the required tools to create the required QoS for PPDR. Ad-hoc networks cannot use this LTE/SAE QoS framework as is. Various mechanisms for QoS provisioning in ad-hoc networks are possible, but may require specific adaptations to comply the PPDR requirements. Unification of infrastructure and ad-hoc networks with respect to QoS should be made by using the same QoS definitions as the LTE infrastructure. This does require that the QoS mechanisms and protocols need to be able to synchronize when communication between nodes of the ad-hoc network and the infrastructure is possible, while the system can continue communication when off-line.

Seamless mobility in heterogeneous networks implies mobility in heterogeneous networks. IP is the unification layer for all services and transport technologies. This layer provides a clearly defined interface both up- and downward in the OSI-stack. IP mobility can be supported by using PMIP. Seamless mobility however requires PFMIP. PFMIP is the technology that executes the handover, where the known IP addresses are pre-requisite. Knowledge on the IP addresses can be created using MIH. Broadcast and multicast are in particular important for PPDR services. This document investigates the multicast extension for PFMIP.

QoS and mobility are two key network aspects that also require management. This document describes the key concepts for network management, including for fault, configuration, accounting, performance and security management. Finally the document describes Network Management System solutions for the various systems including TETRA, LTE, WLAN and ad-hoc networks. A complete NMS description is to be provided in the final version of this document.

BIBLIOGRAPHY

- [1] SALUS Deliverable 2.2, “User Requirements Definition - Intermediate”, December 2014
- [2] SALUS Deliverable 2.4, “User Requirements Definition - Final”, December 2014
- [3] Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture 3GPP TS 23.203 version 10.4.0 Release 10, June 2011
- [4] ITU Radiocommunication Study Groups, “Public Protection and Disaster Relief Communications”, Annex 16 to Document 5A/421-E, 2 December 2013.
- [5] ETSI Technical Report, “Electromagnetic Compatibility and Radio Spectrum Matters (ERM)”, TR 103 102, V.1.1.1, August 2008.
- [6] SALUS Deliverable 5.2, “PPDR Security Architecture, end-to-end security, privacy mechanisms and intrusion detection approach - Intermediate”, January 2015
- [7] ITU Radiocommunication Study Groups, “Radiocommunication Objectives for public protection and disaster relief”, Annex 22 to Document 5A/306-E, 4 June 2013.
- [8] S. Mandold et al. , “IEEE 802.11e Wireless LAN for Quality of Service”, Proceedings of European Wireless (EW2002), Florence, Italy, February 2002.
- [9] LTE poster, Alcatel-Lucent, <http://resources.alcatel-lucent.com/asset/178753>
- [10] 3GPP TS 22.011 – Service Accessibility
- [11] 3GPP TS 23.246 – Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional description
- [12] B. Ishibashi, R. Boutaba, Topology and mobility considerations in mobile ad hoc networks, Elsevier, Ad Hoc Networks 3 (2005) 762–776
- [13] IEEE. 802.11 Standard for Wireless LAN: Medium Access Control (MAC) and Physical Layer (PHY) Specification. (2007). New York: IEEE Inc.
- [14] Lee, S., Ahn, G. S., Zhang, X., & Campbell, A. T. (2000). INSIGNIA: An IP-Based Quality of Service Framework for Mobile Ad Hoc Networks. Journal of Parallel and Distributed Computing, Special issue on Wireless and Mobile Computing and Communications, 60, 374-406.
- [15] Crisostomo, S., Sargento, S., Natkaniec, M., & Vicari, N. (2005). A QoS architecture integrating mobile Ad-Hoc and infrastructure networks. In Proceedings of the ACS/IEEE 2005 international Conference on Computer Systems and Applications (pp. 897-903). Washington, DC: IEEE Computer Society
- [16] Natkaniec, M., Gozdecki, J., & Sargento, S. (2007). A QoS Architecture Integrating Ad-Hoc and Infrastructure in Next Generation Networks. In B. Simak, R. Bestak, & E. Kozowska (Eds.), IFIP International Federation for Information Processing, Personal Wireless Communications (pp. 25–37). New York: Springer.
- [17] Ahn, G. S., Campbell, A., Veres, A., & Sun, L. H. (2002). Supporting Service Differentiation for Real- Time and Best-Effort Traffic in Stateless Wireless Ad Hoc Networks (SWAN). IEEE Transactions on Mobile Computing, 1(3), 192–207.
- [18] He, Y., & Abdel Wahab, H. (2006). HQMM: A Hybrid QoS Model for Mobile Ad-hoc Networks. 11th IEEE Symposium on Computers and Communications, ISCC '06, (pp. 194-200). New York: IEEE Inc.
- [19] Natkaniec, M., Kosek-Szott, K., Szott, S., Gozdecki, J., Głowacz, A., & Sargento, S. (2009). Supporting QoS in Integrated Ad-Hoc Networks. Wireless Personal Communications, Springer, ISSN 1572-834X (Online).

- [20] Lei Chen and W.B. Heinzelman., "QoS-aware routing based on band-width estimation for mobile ad hoc networks" Selected Areas in Communications, IEEE Journal on, 23(3):561-572, March 2005
- [21] M. Conti and S. Giordano "Multihop Ad Hoc Networking: The Reality" Communications Magazine, IEEE, 45(4):88 {95, April 2007.
- [22] H. Yokota, K. Chowdhury, R. Koodli, B. Patil and F. Xia, "Fast Handovers for Proxy Mobile IPv6," RFC 5949, 2010.
- [23] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy mobile ipv6," RFC 5213, 2008.
- [24] R. Wakikawa, S. Gundavelli, Toyota ITC and Cisco, "IPv4 Support for Proxy Mobile IPv6," RFC 5844, 2010.
- [25] T. Schmidt, S. Gao, H. Zhang and M. Waehlich, "Mobile Multicast Sender Support in Proxy Mobile IPv6 (PMIPv6) Domains," RFC 7287, 2014.
- [26] T. Schmidt, M. Waehlich, R. Koodli, G. Fairhurst and D. Liu, "Multicast Listener Extensions for MIPv6 and PMIPv6 Fast Handovers," Internet-Draft, 2014.
- [27] A. Helmy, "A multicast-based protocol for ip mobility support," Proc. Networked Group Communication (NGC2000), pp. 49-58, 2000.
- [28] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas "Protocol Independent Multicast – Sparse Mode (PIMSM): Protocol Specification (Revised)", RFC 4601, August 2006
- [29] C. Wen, C. Wu, and W. Lee, "A context-aware handoff scheme and all-ip mobile multicast service for heterogeneous wireless networks," IEEE Proc. International Conference Ultra Modern Telecommunications & Workshops (ICUMT'09), pp. 1-7, Oct. 2009.
- [30] F. Giust, C. J. Bernardos, S. Figueiredo, P. Neves, T. Melia, "A Hybrid MIPv6 and PMIPv6 Distributed Mobility Management: the MEDIEVAL approach", Mediawin 2011
- [31] F. Siddiqui and S. Zeadally, "Mobility management across hybrid wireless networks: trends and challenges," Computer Communication., vol. 29, pp. 1363-1385, 2006.
- [32] J. Kaippallimalil, R. S. Pazhyannur, P. Yegani, Mapping 802.11 QoS in a PMIPv6 Mobility Domain (draft-kaippallimalil-netext-pmip-qos-wifi-04), 2014
- [33] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2012
- [34] Architecture enhancements for non-3GPP accesses, 3GPP TS 23.402 V9.5.0 (2010-06)
- [35] M. Liebsch, P. Seite, Yokota, J. Korhonen, S. Gundavelli, Quality-of-Service Option for Proxy Mobile IPv6, RFC 7222, May 2014
- [36] Makaya, C., & Pierre, S. (2008). An analytical framework for performance evaluation of ipv6-based mobility management protocols. IEEE Transactions on Wireless Communications, 7(3), 972–983.
- [37] MEDIEVAL Project, Deliverable D4.2 – "IP Multicast Mobility Solutions for Video Services" July 2011
- [38] R Wakikawa, S Gundavelli, IPv4 support for proxy mobile IPv6. IETF RFC5844 (NETLMM Working Group, 2010). <http://tools.ietf.org/html/rfc5844>
- [39] Romdhani, I., Kellil, M., Lach, H. Y., Bouabdallah, A., and Bettahar, H., "IP Mobile Multicast: Challenges and Solutions", IEEE Communications Surveys & Tutorials, 2004
- [40] R. Rummier, A. Gluhak, and A.H. Aghvami, Multicast in Third- Generation Mobile Networks: Services, Mechanisms and Performance. John Wiley and Sons, UK: 2009.
- [41] S. Jeon, N. Kang, and Y. Kim, "Mobility management based on proxy mobile ipv6 for multicasting services in home networks," IEEE Trans. On Consumer Electronics, pp. 1227-1232, Jun. 2009.

- [42] TC Schmidt, S Gao, HK Zhang, M Waehlich, Mobile multicast sender support in proxy mobile IPv6 (PMIPv6) domains, draft-ietf-multimobpmipv6- source-03. IETF Internet Draft (MULTIMOB Working Group, 2013). <http://tools.ietf.org/html/draft-ietf-multimob-pmipv6-source-03>
- [43] TC Schmidt, M Waehlich, S Krishnan, Base deployment for multicast listener support in PMIPv6 domains. IETF RFC 6224 (MULTIMOB Working Group, 2011). <http://tools.ietf.org/html/rfc6224>
- [44] T. Schmidt, M. Waehlich, S. Krishnan, "Base Deployment for Multicast Listener Support in PMIPv6 Domain," RFC 6224, April 2011
- [45] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., & Xia, F. (2010). Fast handovers for proxy mobile ipv6. RFC 5949. <http://tools.ietf.org/html/rfc5949>.
- [46] CISCO, "Network Management Basics," [Online]. Available: http://docwiki.cisco.com/wiki/Network_Management_Basics [on: 05-10-2014].
- [47] CISCO, "Network Management Systems Architectural Leading Practice," [Online]. Available: http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb4c.html [on: 06-10-2014].
- [48] 3GPP TR 36.902, Self-configuring and self-optimizing network (SON) use cases and solutions
- [49] 3GPP TS 32.500, Self-Organizing Networks (SON); Concepts and requirements
- [50] IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services, IEEE, January 2009
- [51] IEEE Std 802.21a-2012, IEEE Standard for Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services (Amendment 1: Security Extensions to Media Independent Handover Services and Protocol), IEEE, May 2012
- [52] B., Fenner, H., Nortel, B., Haberman, & H., Sandick (2006). Multicast Listeners Discovery (MLD)-Based Multicast Forwarding. RFC 4605
- [53] IEEE 802.21-2008, "IEEE Standard for Local and Metropolitan Area Networks— Media Independent Handover Services", Jan. 2009.
- [54] S Gundavelli et al., "Proxy Mobile IPv6", IETF RFC 5213, Aug. 2008.
- [55] 3GPP TS 23.402 V12.3.0 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses", Dec. 2013.
- [56] 3GPP TS 29.275 V12.1.0 "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3", Dec. 2013.
- [57] C.J. Bernardos, "Proxy Mobile IPv6 Extensions to Support Flow Mobility", IETF, draft-ietf-netext-pmipv6-flowmob-08, Oct. 2013

ACRONYMS

#	
3GPP	3 rd Generation Partnership Program
A	
AAA	Authentication, Authorization and Accounting
AC	Access Class
ACL	Access Control Lists
ADDTS	Add Traffic Stream
AF	Application Function
AHQoS	Ad-hoc QoS Controller
AHQoSSig	Ad-hoc QoS Signaling
AMBR	Aggregate MBR
AP	Access Point
APN	Access Point Name
ARQ	Automatic Retransmission reQuest
AS	Application Server
B	
BAU	Business As Usual
BBERF	Bearer Binding and Event Reporting Function
BER	Bit Error Rate
BS-SC	Broadcast and Multicast Service Control
BS	Base Solution
BSS	Basic Service Set

C	
C2	Command and Control
CCC	Command and Control Centre
CCTV	Closed Circuit Television
CN	Corresponding Node
CN	Core Network
CN	Congestion Notification
CND	Congestion Notification Detection
CNM	Congestion Notification Marking
D	
DCN	Data Communications Network
DEA	Diameter Edge Agent
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DLCI	Data Link Connection Identifier
DLP	Direct Link Protocol
DLSW	Data Link Switching Workgroup
DMO	Direct Mode of Operations
DNS	Domain Name Server
DPI	Deep packet Inspection
DR	Designated Router
DSCP	Differentiated Service Control Point

E	
E2E	End to End
EDCA	Enhanced Distributed Channel Access
eNB	evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
ePDG	Evolved Packet Data Gateway
F	
FDDI	Fiber-Distributed Data Interface
FM	Flow Manager
FN	Fragment Number
G	
GPS	Global Positioning System
GRX	GPRS Roaming eXchange
GW	GateWay
H	
HA	Home Agent
HACK	Handover Acknowledgement
HARQ	Hybrid-ARQ
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HQMM	Hybrid QoS Model for Mobile Ad Hoc Networks
HSS	Home Subscriber Subsystem

I	
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv6	Internet Protocol version 6
IPX	IP Exchange
IntServ	Integrated Services
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Information Technology
J	
K	
L	
LMA	Local Mobility Anchor
LTE	Long Term Evolution
LLC	Logical Link Control
M	
MAC	Media Access Control
MAG	Mobile Access Gateway
MANET	Mobile Ad-hoc NETWORK
MAP	Media Aware Proxy

MBMS	Multimedia Broadcast and Multicast System
MBR	Minimum Bit Rate
MCE	MBMS Control Element
MF	More Fragment
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIHU	Media Independent Handover User
MIIS	Media Independent Information Service
MLD	Multicast Listener Discovery
MME	Mobility Management Entity
MLD	Multicast Listener Discovery
MN	Mobile Node
MNO	Mobile Network Operator
MOM	Manager of Managers
MR	Multicast Router
MSDU	MAC Service Data Unit
NSIS	Next Step in Signalling
N	
NAS	Non Access Stratum
NFS	Network File System
NGBR	Non-Guaranteed Bit Rate
nMAG	New MAG
CCC	Command and Control Centre

NMS	Network Management System
NTP	Network Time Protocol
O	
O&M	Operation and Maintenance
OCS	Online Charging System
OFCS	Offline Charging System
OS	Operation System
OSS	Operations Support System
P	
P (bit)	Proactive authentication (bit)
PBA	Proxy Binding Acknowledgement
PBU	Proxy Binding Update
PCF	Point Coordination Function
PCRF	Policy Charging and Rules Function
PERF	Policy Event Reporting Function
PDB	Packet Delay Budget
PDN	Packet Data Network
PDN-GW	Packet Data Network GateWay
PFMIPv6	Proxy Fast Mobile IPv6
PGW	PDN Gateway
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast Sparse Mode
PLMN	Public Land Mobile Network
PLR	Packet Error Loss Rate

pMAG	Previous MAG
PMIP	Proxy Mobile IP
PMIPv6	Proxy Mobile IPv6
PMR	Private Mobile Radio
PoA	Point of Attachment
PoS	Point of Service
PPDR	Public Protection and Disaster Relief
ProSe	Proximity Services
PSK	Pre-Shared Key
Q	
QCI	QoS Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
QoSC	QoS Client
QoSM	QoS Manager
R	
RCND	Received Congestion Notification Detection
RFP	Request For Proposal
RMON	Remote Monitoring
RO	Read-Only
RP	Rendezvous Point
RPx	Reference Point x
RSRB	Remote Source Route Bridging
RW	Read-Write

S	
S (bit)	Security Association (bit)
SAE	Service Architecture Evolution
SAP	Service Access Point
SCTP	Stream Control Transmission Protocol
SDF	Service Data Flow
SGW	Serving Gateway
SIB	System Information Base
SIM	Subscriber Information Module
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SOA	Service Oriented Architecture
SON	Self Optimizing Network
SPR	Subscription Profile Repository
SPT	Shortest Path Tree
SSID	Service Set Identifier
SSM	Source Specific Multicast
SW	Software
SWAN	Stateless Wireless Ad-Hoc Networks
T	
TACACS	Terminal Access Controller Access Control System
TC	Traffic Class
TC	Traffic Controller
TCLAS	Transaction Class

TCP	Transmission Control Protocol
TSPEC	Traffic Specification
TETRA	Terrestrial Trunked Radio Access
TFT	Traffic Flow Template
TLV	Type Length Value
ToS	Type of Service
U	
UDP	User Datagram Protocol
UE	User Equipment
UIR	Unauthenticated Information Request
V	
W	
WCS	Wireless Communications Service
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMM	Wireless Multi Media
X	
Y	
Z	