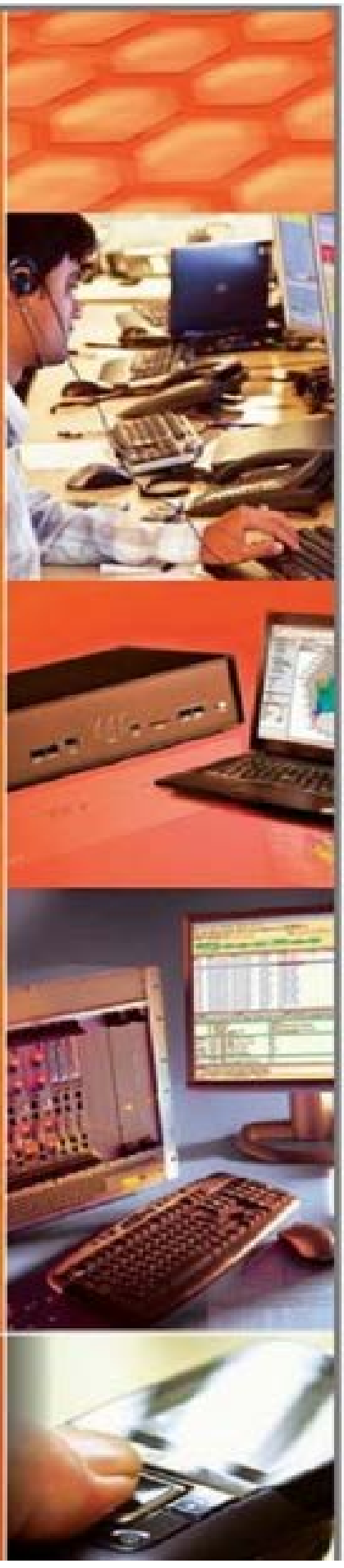
LTE SIGNALING

Troubleshooting & Optimization

RALF KREHER
KARSTEN GAENGER



WILEY

Tektronix
Communications

IPR2024-00138
Petitioners' Ex. 1013
Ex.1013.00001

LTE SIGNALING, TROUBLESHOOTING, AND OPTIMIZATION

LTE Signaling, Troubleshooting and Optimization, First Edition. Ralf Kreher and Karsten Gaenger.
© 2011 John Wiley & Sons, Ltd. Published 2011 by John Wiley & Sons, Ltd.

Ex.1013.00002

LTE SIGNALING, TROUBLESHOOTING, AND OPTIMIZATION

Ralf Kreher and Karsten Gaenger
Both of Tektronix Berlin GmbH, Germany



A John Wiley and Sons, Ltd., Publication

Ex.1013.00003

This edition first published 2011
© 2011 John Wiley & Sons Ltd

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

Kreher, Ralf.
LTE signaling, troubleshooting, and optimization / Ralf Kreher, Karsten Gaenger.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-68900-4 (hardback)
1. Long-Term Evolution (Telecommunications) I. Gaenger, Karsten. II. Title.
TK5103.48325.K74 2011
621.384 – dc22

2010036847

A catalogue record for this book is available from the British Library.

Print ISBN: 978-0-470-68900-4 (H/B)
ePDF ISBN: 978-0-470-97771-2
oBook ISBN: 978-0-470-97772-9
ePub ISBN: 978-0-470-97767-5

Typeset in 9/11pt Times Roman by Laserwords Private Limited, Chennai, India

Ex.1013.00004

Karsten Gaenger

To my lovely lady for her care and patience. To my parents and my sister for being with me and for their continuous support.

As a global standard, LTE might connect more people than ever before. It is my hope that as we increase our ability to communicate we increase our ability to live peaceably together.

Ralf Kreher

I dedicate this book to my grandmother Emilie. She managed to raise four children in the aftermath of World War II after losing her husband, home and all her valuables.

Ex.1013.00005

Contents

Foreword **xi**

Acknowledgments **xiii**

1 Standards, Protocols, and Functions **1**
1.1 LTE Standards and Standard Roadmap 2
1.2 LTE Radio Access Network Architecture 9
1.3 Network Elements and Functions 10
1.3.1 The eNodeB (eNB) 11
1.3.2 Mobility Management Entity (MME) 12
1.3.3 Serving Gateway (S-GW) 12
1.3.4 Packet Data Network Gateway (PDN-GW) 13
1.3.5 Interfaces and Reference Points 13
1.4 Area and Subscriber Identities 17
1.4.1 Domains and Strati 17
1.4.2 IMSI 19
1.4.3 LMSI, TMSI, P-TMSI, M-TMSI, and S-TMSI 20
1.4.4 GUTI 20
1.4.5 IMEI 21
1.4.6 RNTI 22
1.4.7 Location Area, Routing Area, Service Area, Tracking Area, Cell Global Identity 24
1.4.8 Mapping between Temporary and Area Identities for EUTRAN- and UTRAN/GERAN-Based Systems 26
1.4.9 GSM Base Station Identification 27
1.4.10 UTRA Base Station Identification 28
1.4.11 Numbering, Addressing, and Identification in the Session Initiation Protocol 29
1.4.12 Access Point Name 29
1.5 User Equipment 30
1.5.1 UE Categories 31
1.6 QoS Architecture 31
1.7 LTE Security 33
1.8 Radio Interface Basics 38
1.8.1 Duplex Methods 40
1.8.2 Multiple Access Methods 42
1.8.3 OFDM Principles and Modulation 45
1.8.4 Multiple Access in OFDM – OFDMA 48

	1.8.5	*Resource Blocks*	50
	1.8.6	*Downlink Slot Structure*	51
	1.8.7	*OFDM Scheduling on LTE DL*	56
	1.8.8	*SC-FDMA Principles and Modulation*	60
	1.8.9	*Scheduling on LTE UL*	62
	1.8.10	*Uplink Slot Structure*	63
	1.8.11	*Link Adaptation in LTE*	66
	1.8.12	*Physical Channels in LTE*	68
	1.8.13	*Transport Channels in LTE*	78
	1.8.14	*Channel Mapping and Multiplexing*	79
	1.8.15	*Initial UE Radio Access*	80
	1.8.16	*UE Random Access*	81
1.9	LTE Network Protocol Architecture		85
	1.9.1	*Uu – Control/User Plane*	85
	1.9.2	*S1 – Control/User Plane*	86
	1.9.3	*X2 – User/Control Plane*	87
	1.9.4	*S6a – Control Plane*	87
	1.9.5	*S3/S4/S5/S8/S10/S11 – Control Plane/User Plane*	88
1.10	Protocol Functions, Encoding, Basic Messages, and Information Elements		88
	1.10.1	*Ethernet*	88
	1.10.2	*Internet Protocol (IPv4/IPv6)*	89
	1.10.3	*Stream Control Transmission Protocol (SCTP)*	93
	1.10.4	*Radio Interface Layer 2 Protocols*	94
	1.10.5	*Medium Access Control (MAC) Protocol*	95
	1.10.6	*Radio Link Control (RLC) Protocol*	98
	1.10.7	*Packet Data Convergence Protocol (PDCP)*	101
	1.10.8	*Radio Resource Control (RRC) Protocol*	104
	1.10.9	*Non-Access Stratum (NAS) Protocol*	110
	1.10.10	*S1 Application Part (S1AP)*	111
	1.10.11	*User Datagram Protocol (UDP)*	115
	1.10.12	*GPRS Tunneling Protocol (GTP)*	115
	1.10.13	*Transmission Control Protocol (TCP)*	122
	1.10.14	*Session Initiation Protocol (SIP)*	125
	1.10.15	*DIAMETER on EPC Interfaces*	126
2	**E-UTRAN/EPC Signaling**		**131**
2.1	S1 Setup		131
	2.1.1	*S1 Setup: Message Flow*	131
	2.1.2	*S1 Setup: Failure Analysis*	133
2.2	Initial Attach		135
	2.2.1	*Procedure*	135
2.3	UE Context Release Requested by eNodeB		149
	2.3.1	*Procedure*	150
2.4	UE Service Request		152
	2.4.1	*Procedure*	152
2.5	Dedicated Bearer Setup		156
2.6	Inter-eNodeB Handover over X2		157
	2.6.1	*Procedure*	158
2.7	S1 Handover		167
	2.7.1	*Procedure*	170

2.8 Dedicated Bearer Release 179
2.9 Detach 180
2.9.1 Procedure 181
2.10 Failure Cases in E-UTRAN and EPC 183

3 Radio Interface Signaling Procedures 187
3.1 RRC Connection Setup, Attach, and Default Bearer Setup 188
3.1.1 Random Access and RRC Connection Setup Procedure 188
3.1.2 RRC Connection Reconfiguration and Default Bearer Setup 196
3.1.3 RRC Connection Release 205
3.2 Failure Cases 205

4 Key Performance Indicators and Measurements for LTE Radio Network Optimization 209
4.1 Monitoring Solutions for LTE Interfaces 209
4.1.1 Monitoring the Air Interface (Uu) 209
4.1.2 Antenna-Based Monitoring 210
4.1.3 Coax-Based Monitoring 212
4.1.4 CPRI-Based Monitoring 212
4.1.5 Monitoring the E-UTRAN Line Interface 214
4.2 Monitoring the Scheduler Efficiency 218
4.2.1 UL and DL Scheduling Resources 223
4.2.2 X2 Load Indication 224
4.2.3 The eNodeB Layer 2 Measurements 226
4.3 Radio Quality Measurements 227
4.3.1 UE Measurements 230
4.3.2 The eNodeB Physical Layer Measurements 234
4.3.3 Radio Interface Tester Measurements 238
4.3.4 I/Q Constellation Diagrams 238
4.3.5 EVM/Modulation Error Ratio 241
4.4 Control Plane Performance Counters and Delay Measurements 242
4.4.1 Network Accessibility 243
4.4.2 Network Retainability 252
4.4.3 Mobility (Handover) 254
4.5 User Plane KPIs 258
4.5.1 IP Throughput 258
4.5.2 Application Throughput 260
4.5.3 TCP Startup KPIs 263
4.5.4 TCP Round-Trip Time 264
4.5.5 Packet Jitter 264
4.5.6 Packet Delay and Packet Loss on a Hop-to-Hop Basis 265

Acronyms 267

Bibliography 275

Index 277

Foreword

As I watch my children use the latest in video conferencing technology over a mobile handset, I can't help but think of how far we've come. One might recall what the mobile communications industry was like only two decades ago, in the early 1990s. At the time, a considerable portion of the mobile addressable population simply could not comprehend why they would ever need a portable device to originate and receive phone calls. Even more difficult to believe was how this technology would spread through the business world and into the consumer population. After all, the price of a mobile minute was formidable, especially with the general lack of quality of experience and the not-to-be-forgotten 2 kg battery bag we were forced to carry.

In the mid 1990s, 2nd Generation technology was well into its general deployment. As business professionals, we gained acceptance and expectations of a world in which all of our colleagues, customers and suppliers could be reached through ever shrinking mobile devices. The service provider competitive landscape began introducing concepts such as "monthly minutes" while handset subsidization drove mobile communications into the hands of the everyday consumer. Even stranger was seeing the younger population use their thumbs (and not their mouths) to communicate with their friends. Yes, the world of the Short Message Service was taking European and Asian youth by storm.

As we headed towards the end of the century, we began to speak of the concept of Personal Communication Services. The mobile device would become our personal station for all communications, inclusive of data acquisition for business as well as rich entertainment for all users. The mobile device was quickly deemed a portable desktop and portable entertainment system. Well, perhaps a bit overstated at first! Turning the corner of the year 2000, we embraced the introduction of 2.5 Generation technology. Signs of a true portable desktop were emerging. The continuous introduction of additional spectrum for mobile communications, coupled with a now growing consumer thirst for higher bandwidth, accelerated the industry. After massive investments by highly competitive service providers, the uptake of 3rd Generation technology emerged. 3G is now carrying us to where we are today. From my perspective, the age of Personal Communication Service and its much promised devices are now upon us.

Business users can now access and upload office databases through secure wireless connections. Personal users can download music and videos, play online games and, of course, hold discussions over highly sophisticated smartphone devices. All of this has resulted in unprecedented traffic growth over the wireless mobile network and within the mobile core network. Not only is higher bandwidth per device required, but the ability of the network to essentially eliminate latency is also critical in this environment. Hence the birth of the LTE, an end-to-end IP-based architecture fully prepared to deliver these aforementioned requirements. But with LTE comes aspects of increased complexity: a highly intelligent radio interface, now responsible for mobility management, and an enhanced packet core destined to deliver speeds that rival fixed broadband service.

The ability to monitor and troubleshoot the control plane and user plane throughout the radio and core network will be essential to the success of LTE. Tektronix Communications' leadership in testing both the radio interface and the wired interface of the E-UTRAN and Enhanced Packet Core network will allow readers of this book to get a deeper insight into real world call procedures and

Ex.1013.00009

message examples that are unmatched by other publications. Based on Tektronix Communications' experiences and best practices in troubleshooting and optimizing 3G radio access networks, we have already outlined a clear path to what needs to be done to troubleshoot and optimize 4G networks. This book serves as reference for daily work both in the lab and in the field. We also have covered the basics of network architecture and interfaces, protocols and principles of radio interface transmission in a comprehensive way that enables a smooth technology upgrade for all those who already have experience in the 2G and 3G wireless world.

The emphasis of this book is describing the signaling procedures and call flows on the radio interface, in E-UTRAN and within Enhanced Packet Core networks. We discuss the most common failure scenarios for live network troubleshooting. We also highlight essential performance measurement counters and define industry-adopted KPIs for *accessibility, retainability and mobility*. A large section covers in detail how to measure radio and user plane quality, especially over the air interface. All of this includes practical examples from Tektronix Communications measuring equipment, the radio interface tester K2Air and the Network and Service Analyzer platform NSA.

We are confident that this book will provide an exceptional reference for a broad range of individuals interested in next-generation mobile communications. Whether you are a highly advanced mobile network engineer or a student seeking an introduction to 3G LTE networks, you will benefit from continued accessibility to this reference. Please enjoy.

Richard Kenedi
Vice President and General Manager
Tektronix Communications
Test and Optimization Product Line

Acknowledgments

We would like to take the chance to acknowledge the efforts of all who participated directly or indirectly in creating and publishing this book.

First of all, a special "thank you" goes to Ralf Kreher's sister Brit who created and formatted all the figures you will find in this book. Another one goes to our family members and all who supported and encouraged us to get this work done.

Eiko Seidel and his team at Nomor Research have not just created some excellent primers about LTE radio interface procedures and set up the 3GPP LTE Standards Group at www.linkedin.com, but also given us deep insight into their scheduling simulator, a tool used to design scheduling algorithms for eNodeB vendors.

Antonio Bovo working as System Architect for Tektronix Padova contributed some very detailed research on E-UTRAN protocols and functions. From his work we have derived the major part of the S1AP section of this book.

Karsten Gienskey and Marcus Garin working for Tektronix Berlin shared with us their earliest prototypes and design specifications for RLC reassembly and radio interface tracing. Without their great job we would have been "blind" on the radio interface.

Ulrich Jeczawitz, freelancer and ex-colleague of Tektronix Berlin, and the development team of the Tektronix G35 protocol simulator led by Dirk-Holger Lenz, generated traces of E-UTRAN and Enhanced Packet Core signaling procedures long before they occurred in any live network field trial.

Lars Chudzinsky, working on LTE call trace for Tektronix Berlin, contributed design specifications of protocol failure events that became the raw material for Section 2.10.

This book would not exist without the ideas, questions, and requirements contributed by customers, colleagues, and subcontractors. Besides all the others who cannot be named personally, we would like to express our thanks especially to the following people: Jürgen Forsbach, Andre Huge, Steffen Hülpüsch, Armin Klopfer, and Jens Plogsties.

In addition, our thanks go to the Management of the Tektronix Communications Test & Optimization Product Line, in particular the Human Resources Department represented by Marion Kaehlke and R&D Berlin Director Jens Dittrich who supported the idea of writing this book and approved the usage of Tektronix Communications material in the contents.

Maïssa Bahsoun and Jeanne Lancry-Gulino have been our prime contacts in 3GPP in obtaining copyright permissions and, last but not least, we also would like to express our thanks to the team at John Wiley & Sons, Ltd, especially Mark Hammond, Sarah Tilley, and Sophia Travis, for their strong support.

Ralf Kreher and Karsten Gaenger
Berlin, 1 July 2010

1

Standards, Protocols, and Functions

LTE (Long-Term Evolution) of UMTS (Universal Mobile Telecommunications Service) is one of the latest steps in an advancing series of mobile telecommunication systems. The standards body behind the paperwork is the 3rd Generation Partnership Project (3GPP).

Along with the term LTE, the acronyms EPS (Evolved Packet System), EPC (Evolved Packet Core), and SAE (System Architecture Evolution) are often heard. Figure 1.1 shows how these terms are related to each other: EPS is the umbrella that covers both the LTE of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the SAE of the EPC network.

LTE was and is standardized in parallel to other radio access network technologies like EDGE (Enhanced Data Rates for GSM evolution) and HSPA (High-Speed Packet Access). This means that LTE is not a simple replacement of existing technologies. Rather it is expected that different kinds of radio access will coexist in operator networks.

From this background it emerges that understanding LTE also requires understanding alternative and coexisting technologies. Indeed, one of the major challenges of LTE signaling analysis will concern the analysis of handover procedures. Especially, the options for possible inter-RAT (Radio Access Technology) handovers have multiplied compared to what was possible in UMTS Release 99. However, also intra-system handover and dynamic allocation of radio resources to particular subscribers will play an important role.

The main drivers for LTE development are:

- reduced delay for connection establishment;
- reduced transmission latency for user plane data;
- increased bandwidth and bit rate per cell, also at the cell edge;
- reduced costs per bit for radio transmission;
- greater flexibility of spectrum usage;
- simplified network architecture;
- seamless mobility, including between different radio access technologies;
- reasonable power consumption for the mobile terminal.

It must be said that LTE as a radio access technology is flanked by a couple of significant improvements in the core network known as the EPS. Simplifying things a little, it is not wrong to state that EPS is an all-IP (Internet Protocol) transport network for mobile operators. IP will also become the physical transport layer on the wired interfaces of the E-UTRAN. This all-IP architecture is also one of the facts behind the bullet point on simplified network architecture. However, to assume that to

LTE Signaling, Troubleshooting and Optimization, First Edition. Ralf Kreher and Karsten Gaenger.
© 2011 John Wiley & Sons, Ltd. Published 2011 by John Wiley & Sons, Ltd.

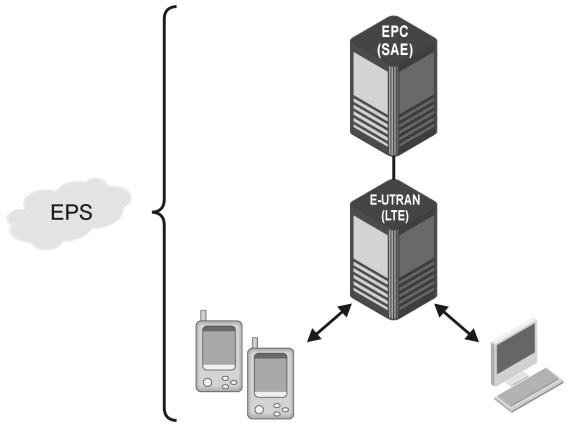


Figure 1.1 EPC and LTE under the umbrella of EPS.

be familiar with the TCP/IP world is enough to understand and measure LTE would be a fatal error. While the network architecture and even the basic signaling procedures (except the handovers) become simpler, the understanding and tracking of radio parameters require more knowledge and deeper investigation than they did before. Conditions on the radio interface will change rapidly and with a time granularity of 1 ms the radio resources assigned to a particular connection can be adjusted accordingly.

For instance, the radio quality that is impacted by the distance between the User Equipment (UE) and base station can determine the modulation scheme and, hence, the maximum bandwidth of a particular connection. Simultaneously, the cell load and neighbor cell interference – mostly depending on the number of active subscribers in that cell – will trigger fast handover procedures due to changing the best serving cell in city center areas, while in rural areas macro cells will ensure the best possibley coverage.

The typical footprint of a LTE cell is expected by 3GPP experts to be in the range from approximately 700 m up to 100 km. Surely, due to the wave propagation laws such macro cells cannot cover all services over their entire footprint. Rather, the service coverage within a single cell will vary, for example, from the inner to the outer areas and the maximum possible bit rates will decline. Thus, service optimization will be another challenge, too.

1.1 LTE Standards and Standard Roadmap

To understand LTE it is necessary to look back at its predecessors and follow its path of evolution for packet switched services in mobile networks.

The first stage of the General Packet Radio Service (GPRS), that is often referred to as the 2.5G network, was deployed in live networks starting after the year 2000. It was basically a system that offered a model of how radio resources (in this case, GSM time slots) that had not been used by Circuit Switched (CS) voice calls could be used for data transmission and, hence, profitability of the network could be enhanced. At the beginning there was no pre-emption for PS (Packet Switched) services, which meant that the packet data needed to wait to be transmitted until CS calls had been finished.

In contrast to the GSM CS calls that had a Dedicated Traffic Channel (DTCH) assigned on the radio interface, the PS data had no access to dedicated radio resources and PS signaling, and the payload was transmitted in unidirectional Temporary Block Flows (TBFs) as shown in Figure 1.2.

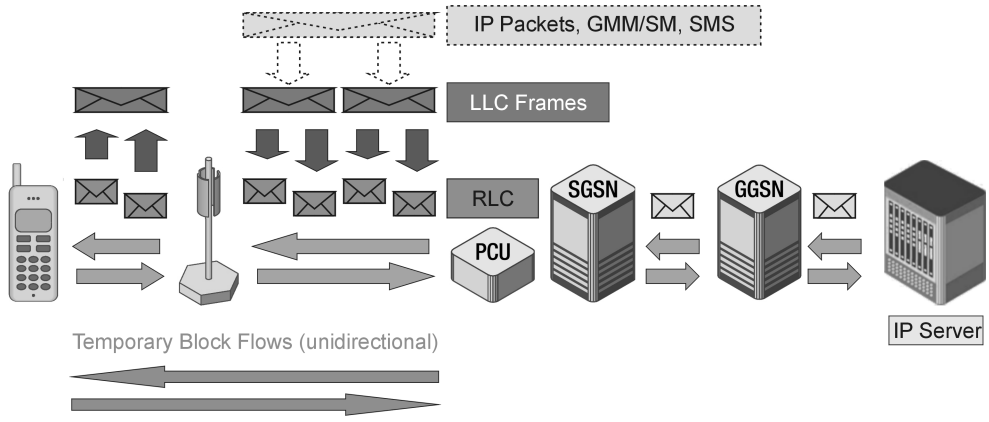


Figure 1.2 Packet data transfer in 2.5G GPRS across Radio and Abis interfaces.

These TBFs were short and the size of data blocks was small due to the fact that the blocks must fit the transported data into the frame structure of a 52-multiframe, which is the GSM radio transmission format on the physical layer. Larger Logical Link Control (LLC) frames that contain already segmented IP packets needed to be segmented into smaller Radio Link Control (RLC) blocks.

The following tasks are handled by the RLC protocol in 2.5G:

- Segmentation and reassembly of LLC packets → segmentation results in RLC blocks.
- Provision of reliable links on the air interface → control information is added to each RLC block to allow Backward Error Correction (BEC).
- Performing sub-multiplexing to support more than one MS (Mobile Station) by one physical channel.

The Medium Access Control (MAC) protocol is responsible for:

- point-to-point transfer of signaling and user data within a cell;
- channel combining to provide up to eight physical channels to one MS;
- mapping RLC blocks onto physical channels (time slots).

As several subscribers can be multiplexed on one physical channel, each connection has to be (temporarily) uniquely identified. Each TBF is identified by a Temporary Flow Identifier (TFI). The TBF is unidirectional (uplink (UL) and downlink (DL)) and is maintained only for the duration of the data transfer.

Toward the core network in 2.5G GPRS the Gb interface is used to transport the IP payload as well as GPRS Mobility Management/Session Management (GMM/SM) signaling messages and short messages (Short Message Service, SMS) between SGSN and the PCU (Packet Control Unit) – see Figure 1.3. The LLC protocol is used for peer-to-peer communication between SGSN and the MS and provides acknowledged and unacknowledged transport services. Due to different transmission conditions on physical layers (E1/T1 on the Gb and Abis interfaces, 52-multiframe on the Air interface), the size of IP packets needs to be adapted. The maximum size of the LLC payload field is 1540 octets (bytes) while IP packets can have up to 65 535 octets (bytes). So the IP frame is segmented on SGSN before transmission via LLC and reassembled on the receiver side.

All in all, the multiple segmentation/reassembly of IP payload frames generates a fair overhead of transport header information that limits the chargeable data throughput. In addition, the availability of

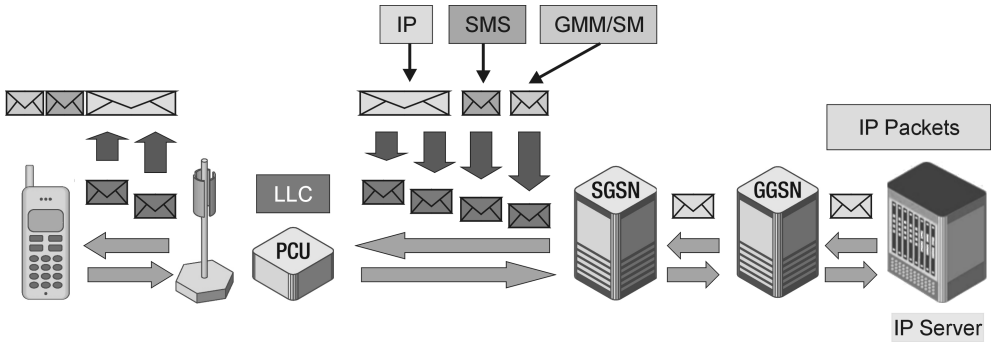


Figure 1.3 Packet data transfer in 2.5G GPRS.

radio resources for PS data transport has not been guaranteed. So this system was only designed for non-real-time services like web-browsing or e-mail.

To overcome these limitations the standards organizations proposed a set of enhancements that led to the parallel development of UMTS and EGPRS (Enhanced GPRS) standards. The most successful EGPRS standard that is found today in operators' networks is the EDGE standard. From the American Code Division Multiple Access (CDMA) technology family another branch of evolution led to the CDMA2000 standards (defined by the 3GGP2 standards organization), but since the authors have not seen any interworking between CDMA2000 and Universal Terrestrial Radio Access Network (UTRAN) or GSM/EDGE Radio Access Network (GERAN) so far, this technology will not be discussed further in this book.

The most significant enhancements of EGPRS compared to GSM/GPRS are shown in Figures 1.4 and 1.5. On the one hand a new modulation technique, 8 Phase Shift Keying (8PSK), was introduced to allow transmission of 8 bits per symbol across the air interface and, thus, an increase in the maximum possible bit rate from 20 to 60 kbps. On the other hand, to use the advantages of the new 8PSK modulation technique it was necessary to adapt the data format on the RLC/MAC layer, especially regarding the size of the transport blocks and the time transmission interval of the transport blocks. Different transport block formats require a different CS. Thus, the so-called Modulation and Coding Scheme (MCS) and CS for GPRS and EGPRS as shown in Figure 1.4 have been defined. These MCSs

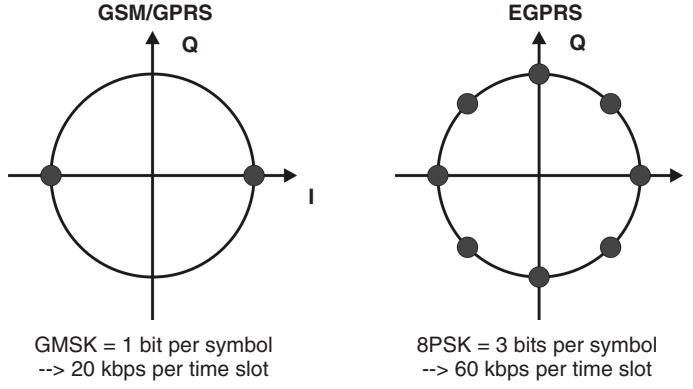


Figure 1.4 GSM/GPRS vs. EGPRS modulation.

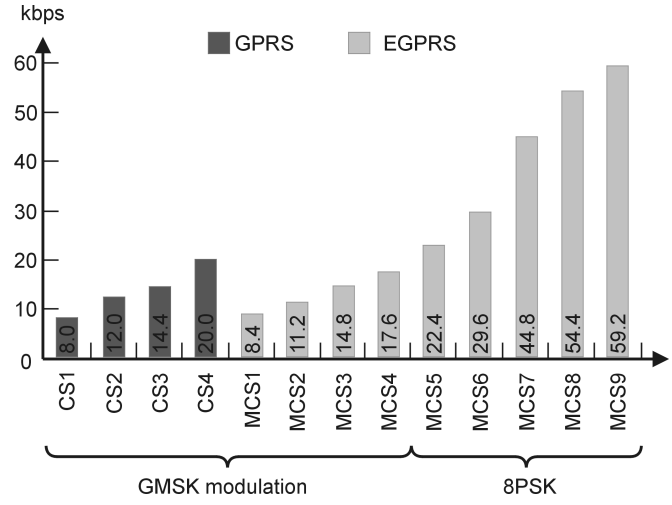


Figure 1.5 Modulation/coding scheme and maximum bit rate in GSM/GPRS vs. EGPRS.

stand for defined radio transmission capabilities on the UE and BTS (Base Transceiver Station) side. It is important to mention this, because in a similar way capability definition with UE physical layer categories instead of MCS were introduced for HSPA and will be found in LTE again.

In comparison to GSM/GPRS, the EGPRS technology also offered a more efficient retransmission of erroneous data blocks, mostly with a lower MCS than the one used previously. The retransmitted data also does not need to be sent in separate data blocks, but can be appended piece by piece to present regular data frames. This highly sophisticated error correction method, which is unique for EGPRS, is called Incremental Redundancy or Automatic Repeat Request (ARQ) II and is another reason why higher data transmission rates can be reached using EGPRS.

As a matter of fact, as shown in Figure 1.6, the risk of interference and transmission errors becomes much higher when the distance between a base station and a UE is large. Consequently, the MCS that allows the highest maximum bit rate cannot be used in the overall cell coverage area, but only in a smaller area close to the base station's antenna. Also for this specific behavior, an adequate expression will be found in LTE radio access.

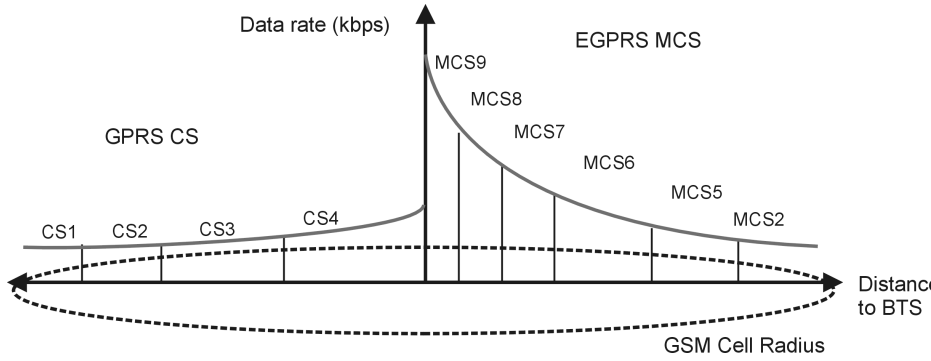


Figure 1.6 Cell footprint of maximum bit rate as function of MCS in (E)GPRS.

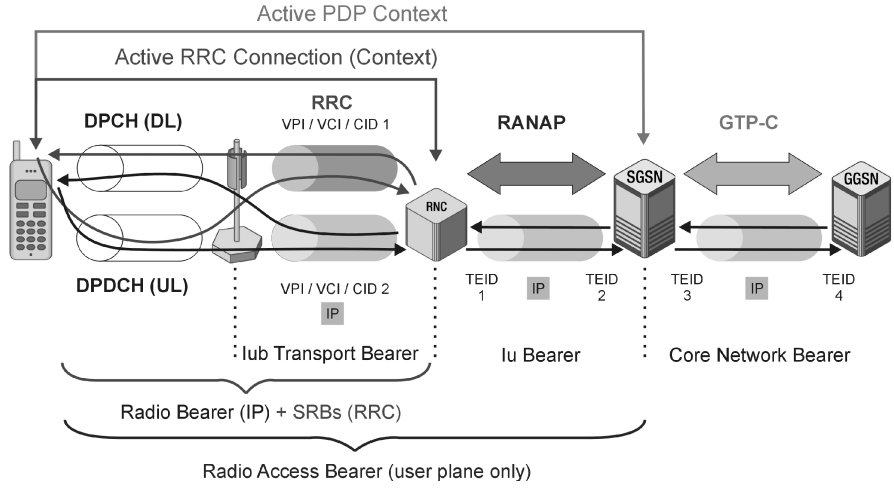


Figure 1.7 IP payload transmission using Release 99 bearers with UE in CELL_DCH state.

Since these early days two key parameters have driven the evolution of packet services further toward LTE: higher data rates and shorter latency. EGPRS (or EDGE) focused mostly on higher bit rates, but did not include any latency requirements or algorithms to guarantee a defined Quality of Service (QoS) in early standardization releases. Meanwhile, in parallel to the development of UMTS standards, important enhancements to EDGE have been defined that allow pre-emption of radio resources for packet services and control of QoS. Due to its easy integration in existing GSM networks, EDGE is widely deployed today in cellular networks and is expected to coexist with LTE on the long haul.

Nevertheless, the first standard that promised complete control of QoS was UMTS Release 99. In contrast to the TBFs of (E)GPRS, the user is assigned dedicated radio resources for PS data that are permanently available through a radio connection. These resources are called bearers.

In Release 99, when a PDP (Packet Data Protocol) context is activated the UE is ordered by the RNC (Radio Network Controller) to enter the Radio Resource Control (RRC) CELL_DCH state. Dedicated resources are assigned by the Serving Radio Network Controller (SRNC): these are the dedicated physical channels established on the radio interface. Those channels are used for transmission of both IP payload and RRC signaling – see Figure 1.7. RRC signaling includes the exchange of Non-Access Stratum (NAS) messages between the UE and SGSN.

The spreading factor of the radio bearer (as the combination of several physical transport resources on the Air and Iub interfaces is called) depends on the expected UL/DL IP throughput. The expected data transfer rate can be found in the RANAP (Radio Access Network Application Part) part of the Radio Access Bearer (RAB) assignment request message that is used to establish the Iu bearer, a GPRS Tunneling Protocol (GTP) tunnel for transmission of a IP payload on the IuPS interface between SRNC and SGSN. While the spreading factor controls the bandwidth of the radio connection, a sophisticated power control algorithm guarantees the necessary quality of the radio transmission. For instance, this power control ensures that the number of retransmitted frames does not exceed a certain critical threshold.

Activation of PDP context results also in the establishment of another GTP tunnel on the Gn interface between SGSN and GGSN. In contrast to IuPS, where tunnel management is a task of RANAP, on the Gn interface – as in (E)GPRS – the GPRS Tunneling Protocol – Control (GTP-C) is responsible for context (or tunnel) activation, modification, and deletion.

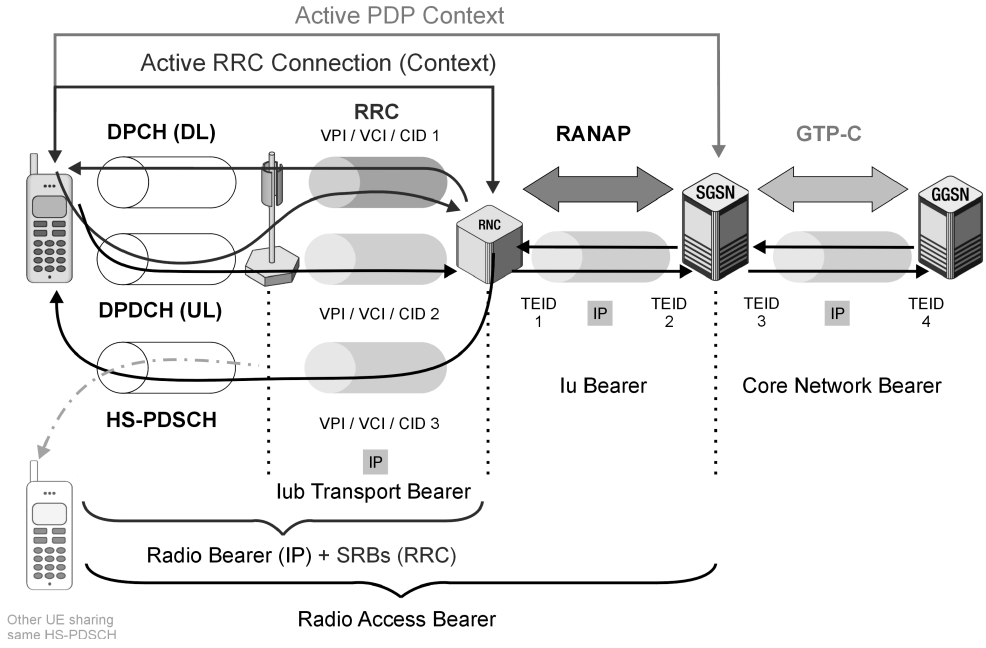


Figure 1.8 IP data transfer using HSDPA.

However, in Release 99 the maximum possible bit rate is still limited to 384 kbps for a single connection and, more dramatically, the number of users per cell that can be served by this highest possible bit rate is very limited (only four simultaneous 384 kbps connections per cell are possible on the DL due to the shortness of DL spreading codes).

To increase the maximum possible bit rate per cell as well as for the individual user, HSPA was defined in Releases 5 and 6 of 3GPP.

In High-Speed Downlink Packet Access (HSDPA) the High-Speed Downlink Shared Channel (HS-DSCH) which bundles several High-Speed Physical Downlink Shared Channels (HS-PDSCHs) is used by several UEs simultaneously – that is why it is called a shared channel.

A single UE using HSDPA works in the RRC CELL_DCH state. For DL payload transport the HSDSCH is used, that is, mapped onto the HS-PDSCH. The UL IP payload is still transferred using a dedicated physical data channel (and appropriate Iub transport bearer); in addition, the RRC signaling is exchanged between the UE and RNC using the dedicated channels – see Figure 1.8.

All these channels have to be set up and (re)configured during the call. In all these cases both parties of the radio connection, cell and UE, have to be informed about the required changes. While communication between NodeB (cell) and CRNC (Controlling Radio NetworkController) uses NBAP (Node B Application Part), the connection between the UE and SRNC (physically the same RNC unit, but different protocol entity) uses the RRC protocol.

The big advantage of using a shared channel is higher efficiency in the usage of available radio resources. There is no limitation due to the availability of codes and the individual data rate assigned to a UE can be adjusted quicker to the real needs. The only limitation is the availability of processing resources (represented by channel card elements) and buffer memory in the base station.

In 3G networks the benefits of an Uplink Shared Channel (UL-SCH) have not yet been introduced due to the need for UL power control, that is, a basic constraint of Wideband CDMA (WCDMA)

networks. Hence, the UL channel used for High-Speed Uplink Packet Access (HSUPA) is an Enhanced Dedicated Channel (E-DCH). The UL transmission data volume that can be transmitted by the UE on the UL is controlled by the network using so-called "grants" to prevent buffer overflow in the base station and RNC. The same "grant" mechanism will be found in LTE.

All in all, with HSPA in the UTRAN the data rates on the UL and DL have been significantly increased, but packet latency is still a critical factor. It takes quite a long time until the RRC connection in the first step and the radio bearer in the second step are established. Then, due to limited buffer memory and channel card resources in NodeB, an often quite progressive settings of user inactivity timers leads to transport channel-type switching and RRC state change procedures that can be summarized as intra-cell hard handovers. Hard handovers are characterized by the fact that the active radio connection including the radio bearer is interrupted for a few hundred milliseconds. Similar interruptions of the data transmission stream are observed during serving HSDPA cell change procedures (often triggered by a previous soft handover) due to flushing of buffered data in NodeB and rescheduling of data to be transmitted by the RNC. That such interruptions (occurring in dense city center areas with a periodicity of 10–20 seconds) are a major threat for delay-sensitive services is self-explanatory.

Hence, from the user plane QoS perspective the two major targets of LTE are:

- a further increase in the available bandwidth and maximum data rate per cell as well as for the individual subscriber;
- reducing the delays and interruptions in user data transfer to a minimum.

These are the reasons why LTE has an always-on concept in which the radio bearer is set up immediately when a subscriber is attached to the network. And all radio resources provided to subscribers by the E-UTRAN are shared resources, as shown in Figure 1.9. Here it is illustrated that the IP payload as well as RRC and NAS signaling are transmitted on the radio interfaces using unidirectional shared channels, the UL-SCH and the Downlink Shared Channel (DL-SCH). The payload part of this radio connection is called the radio bearer. The radio bearer is the bidirectional point-to-point connection for the user plane between the UE and eNodeB (eNB). The RAB is the user plane connection between

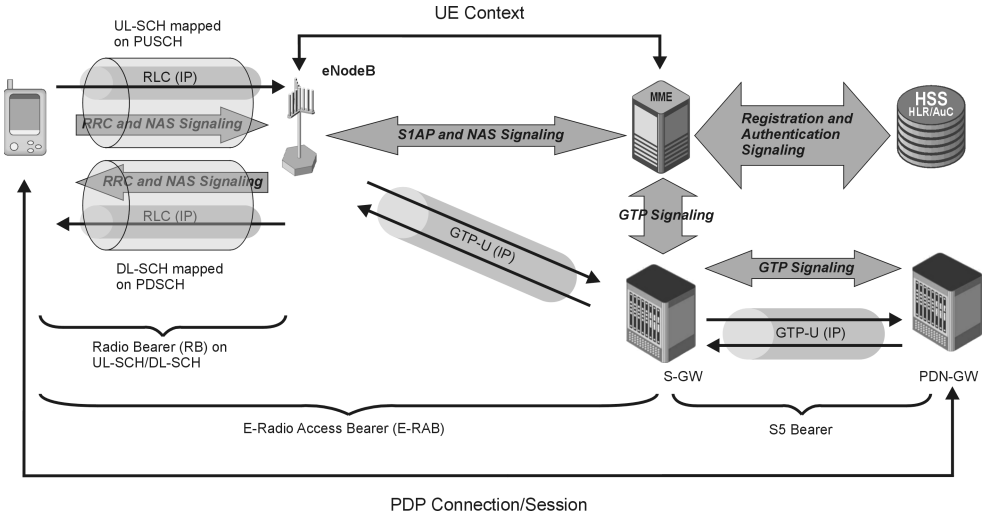


Figure 1.9 Packet data transfer in E-UTRAN/EPC.

the UE and the Serving Gateway (S-GW) and the S5 bearer is the user plane connection between the S-GW and public data network gateway (PDN-GW).

Note that a more detailed explanation of the LTE/EPC bearer concept is given in Section 1.6 of this chapter.

The end-to-end connection between the UE and PDN-GW, that is, the gateway to the IP world outside the operator's network, is called a PDN connection in the E-UTRAN standard documents and a session in the core network standards. Regardless, the main characteristic of this PDN connection is that the IP payload is transparently tunneled through the core and the radio access network.

To control the tunnels and radio resources a set of control plane connections runs in parallel with the payload transport. On the radio interface RRC and NAS signaling messages are transmitted using the same shared channels and the same RLC transport layer that is used to transport the IP payload.

RRC signaling terminates in the eNB (different from 3G UTRAN where RRC was transparently routed by NodeB to the RNC). The NAS signaling information is – as in 3G UTRAN – simply forwarded to the Mobility Management Entity (MME) and/or UE by the eNB.

For registration and authentication the MME exchanges signaling messages with the central main subscriber databases of the network, the Home Subscriber Server (HSS).

To open, close, and modify the GTP/IP tunnel between the eNB and S-GW, the MME exchanges GTP signaling messages with the S-GW and the S-GW has the same kind of signaling connection with the PDN-GW to establish, release, and maintain the GTP/IP tunnel called the S5 bearer.

Between the MME and eNB, together with the E-RAB, a UE context is established to store connection-relevant parameters like the context information for ciphering and integrity protection. This UE context can be stored in multiple eNBs, all of them belonging to the list of registered tracking areas for a single subscriber. Using this tracking area list and UE contexts, the inter-eNB handover delay can be reduced to a minimum.

The two most basic LTE standard documents are 3GPP 23.401 "GPRS Enhancements for E-UTRAN Access" and 3GPP 36.300 "Overall Description Evolved Universal Terrestrial Radio Access (E-UTRA) and E-UTRAN." These two specs explain in a comprehensive way the major improvements in LTE that are pushed by an increasing demand for higher bandwidth and shorter latency of PS user plane services. The basic network functions and signaling procedures are explained as well as the network architecture, interfaces, and protocol stacks.

Although this book will not become simply a copy of what is already described in the standard documents, it is necessary to give a summary of the facts and parameters that are required to understand the signaling procedures and key performance indicators of the network and services. Additional explanations will be given to highlight facts that cannot be found in the specs.

1.2 LTE Radio Access Network Architecture

The E-UTRAN comes with a simple architecture that is illustrated in Figure 1.10. The base stations of the network are called eNodeB and each eNB is connected to one or multiple MMEs. These MMEs in turn are connected to a S-GW that may also be co-located (comprising the same physical hardware) with the MME. The interface between the eNB and MME is the called the S1 interface. In case the MME and S-GW are not found in the same physical entity, the S1 control plane interface (S1-MME) will connect the eNB and MME while the S1 user plane interface (here S1-U) will connect the eNB with the S-GW.

In case one eNB is connected to multiple MMEs, these MMEs form a so-called MME pool and the appropriate network functionality is called S1 flex. The initial signaling procedure used to connect an eNB with a MME is the S1 setup procedure of the S1 Application Part (S1AP).

The X2 interface is used to connect eNBs with each other. The main purpose of this connectivity is intra-E-UTRAN handover. In the real world it will not be possible for all eNBs of the network to be

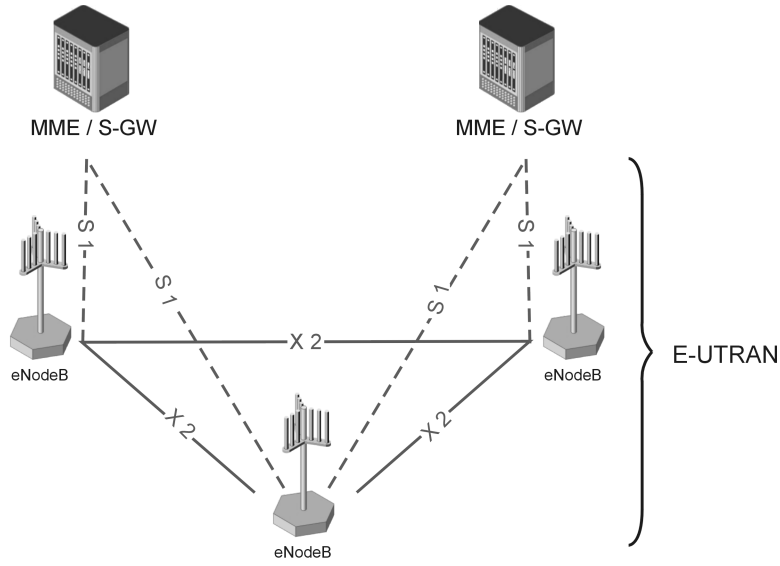


Figure 1.10 E-UTRAN network architecture (according to 3GPP 36.300). Reproduced with permission from © 2008 3GPP™.

connected via X2 due to limited transport resources on the wired interfaces. It also must be expected that, physically, the X2 links will lead from one eNB to the MME and then back to a second eNB. In other words, the hubs will be located at the physical location of the MME.

It is important to understand that only the base stations and their physical connections (wires or fibers) are defined by 3GPP as the E-UTRAN, while MME and S-GW are seen as elements of the EPC network.

1.3 Network Elements and Functions

The explanation given in the previous section indicates that, compared to base stations in GSM and UMTS UTRAN, the eNB will cover a set of new functions that are crucial to understand how the E-UTRAN is working.

In addition, the functionality of the MME and S-GW is different from that of their 2G/3G relatives, the RNC and the SGSN.

The following list of logical meta-functions performed within the overall network/system was defined by 3GPP:

- Network access control functions.
- Packet routing and transfer functions.
- Mobility management functions.
- Security functions.
- Radio resource management functions.
- Network management functions.

These meta-functions are found in the different network elements with a more specific functionality definition.

1.3.1 The eNodeB (eNB)

The eNB is the network entity that is responsible for radio interface transmission and reception. This includes radio channel modulation/demodulation as well as channel coding/decoding and multiplexing/demultiplexing.

System information is broadcast in each cell on the radio interface DL to provide basic information to UEs as a prerequisite to access the network.

The LTE base station hosts all RRC functions such as broadcast of system information and RRC connection control including:

- Paging of subscribers.
- Establishment, modification, and release of RRC connection including the allocation of temporary UE identities (Radio Network Temporary Identifier, RNTI).
- Initial security activation, which means the initial configuration of the Access Stratum (AS) integrity protection for the control plane and AS ciphering for both control plane and user plane traffic.
- RRC connection mobility that includes all types of intra-LTE handover (intra-frequency and inter-frequency). In the case of handover, the source eNB will take care of the associated security handling and provide the necessary key and algorithm information to the handover target cell by sending specific RRC context information embedded in a transparent container to the handover target eNB.
- Establishment, modification, and release of DRBs (Dedicated Radio Bearers) carrying user data.
- Radio configuration control, especially the assignment and modification of ARQ and Hybrid Automatic Repeat Request (HARQ) parameters as well as Discontinuous Reception (DRX) configuration parameters.
- QoS control to ensure that, for example, user plane packets of different connections are scheduled with the required priority for DL transmission and that mobiles receive the scheduling grants for UL data transmission according to the QoS parameters of the radio bearers.
- Recovery functions that allow re-establishment of radio connections after physical channel failure or Radio Link Control Acknowledged Mode (RLC AM) retransmission errors.

The most crucial part for measuring the eNB performance is the UL/DL resource management and packet scheduling performed by the eNB. This is probably the most difficult function which requires the eNB to cope with many different constraints like radio link quality, user priority, requested QoS, and UE capabilities. It is the task of the eNB to make use of the available resources in the most efficient way.

Furthermore, the RRC entity of the eNB covers all types of intra-LTE and inter-RAT measurements, in particular:

- Setup, modification, and release of measurements for intra-LTE intra-frequency, intra-LTE inter-frequency, inter-RAT mobility, transport channel quality, UE internal measurement reports to indicate, for example, current power consumption and GPS positioning reports sent by the handset.
- For compressed mode measurements it is necessary to configure, activate, and deactivate the required measurement gaps.
- The evaluation of reported measurement results and start of necessary handover procedures are also eNB functions (while in 3G UMTS all measurement evaluation and handover control functions have been embedded in the RNC). The many different parameters used in RRC measurement control functions like hysteresis values, time to trigger timer values, and event level threshold of RSRP and RSRQ (Received Signal Reference Power and Received Signal Reference Quality) are the focus of radio network optimization activities.

Other functions of the eNB comprise the transfer of dedicated NAS information and non-3GPP dedicated information, the transfer of UE radio access capability information, support for E-UTRAN

sharing (multiple Public Land Mobile Network (PLMN) identities), and management of multicast/broadcast services.

The support of self-configuration and self-optimization is seen as one of the key features of the E-UTRAN. Among these functions we find, for example, intelligent learning functions for automatic updates of neighbor cell lists (handover candidates) as they are used for RRC measurement tasks and handover decisions.

The eNB is a critical part of the user plane connections. Here the data is routed, multiplexed, ciphered/deciphered, segmented, and reassembled. It is correct to say that on the E-UTRAN transport layer level, the eNB acts as an IP router and switch. The eNB is also responsible for optional IP header compression. On the control plane level, the eNB selects the MME to which NAS signaling messages are routed.

1.3.2 Mobility Management Entity (MME)

The MME is responsible for the NAS connection with the UE. All NAS signaling messages are exchanged between the UE and MME to trigger further procedures in the core network if necessary.

A new function of the E-UTRAN is NAS signaling security. The purpose of this feature is to protect the signaling messages that could reveal the true subscriber's identity and location from unauthorized eavesdropping.

The MME is also responsible for paging subscribers in the EPS Connection Management (ECM) IDLE state (including control and execution of paging retransmission) and is concerned with tracking area list management. The list of tracking areas is the list of locations where the UE will be paged.

To route the user plane data streams the MME will select the best fitting PDN-GW and S-GW. It will also connect the E-UTRAN with the 3G UTRAN using the S3 interface (MME to SGSN). When necessary, a relocation of gateways will be triggered and controlled by the MME.

As its name suggests, the MME will perform management of handovers by selecting a new (target) MME or SGSN for handovers to 2G or 3G 3GPP access networks. Also, it is the MME that hosts the connection to the HSS across the S6a interface and, hence, it is responsible for roaming management and authentication of subscribers.

Last but not least, the MME sets up, modifies, and releases default and dedicated bearers. This function is commonly known as the bearer management function.

According to standard documents, the MME will allow lawful interception of signaling traffic and transfer of warning messages (including selection of an appropriate eNB). The purpose of warning message transfer is to inform people living in a larger area about upcoming natural disasters like storms, bush fires, or tsunamis.

1.3.3 Serving Gateway (S-GW)

The S-GW is the gateway which terminates the interface to the E-UTRAN. A particular LTE subscriber will always be connected by a single S-GW.

In the case of inter-eNB handover, the S-GW acts as the mobility anchor of the connection and remains the same while the path for the transport of signaling and user plane will be switched onto the S1 interface. Once a handover is executed successfully and the associated UE has left the S-GW, the old S-GW will send one or more "end marker" packets to the source eNB, source SGSN, or source RNC of the handover to assist the reordering of user plane packets in these network elements.

Mobility anchoring of the S-GW is also defined for inter-3GPP mobility. Here the S-GW acts as the terminating point of the S4 interface (see Chapter 2 for interface definitions and figures) and routes the traffic between the 2G/3G SGSN and the PDN-GW of the EPC. In other words, when it comes to inter-RAT handover involving the S4 interface, the S-GW acts as the Gateway GPRS Support Node

(GGSN) (of the 2G/3G PS core network) that enables usage of the EPC transport and functions for UTRAN/GERAN PS services.

If the UE is in ECM-IDLE mode (see Section 1.10.9 for a description of different NAS states) the S-GW buffers user plane packets that will be sent to the UE after a successful paging response. The paging via the S1 and Uu interfaces is also triggered by the S-GW.

The S-GW is the network element that provides connectivity and software implementations for lawful interception.

On the IP transport layer the S-GW acts as a packet router. User plane packets are forwarded transparently in the UL and DL direction and their underlying transport units are marked by S-GW with parameters like DiffServ Code Point, based on the QoS Class Indicator (QCI) of the associated EPS bearer.

Also embedded in the S-GW software are various charging functions for UL and DL charging per UE, PDN, and QCI. These functions are used to charge the operator's own subscribers as well as roaming users (inter-operator charging).

The S-GW can be connected to SGSNs in non-roaming and roaming scenarios. However, connectivity to a GGSN is not supported.

1.3.4 Packet Data Network Gateway (PDN-GW)

The PDN-GW provides access from the mobile operator's network to the PS networks that host the payload contents and operator's IP services. If a user has access to more than one packet data network it is possible that this user is connected to more than just one PDN-GW. It is not possible for the same UE to simultaneously open connections to a PDN-GW and to a GGSN in the 3G PS domain, according to 3GPP standards.

The main function of the PDN-GW is to establish, maintain, and delete GTP tunnels to S-GW or SGSN in the case of inter-RAT mobility scenarios. The PDN-GW allocates the user's dynamic IP addresses and routes the user plane packets. In addition, it provides functions for lawful interception, policy/QoS control, and charging.

For policy control and charging, the PDN-GW can be connected to a Policy and Charging Rule Function (PCRF) via the Gx reference point. The PCRF provides guidance on how a particular service data flow should be treated in terms of priority, throughput, and other QoS parameters according to the user's subscription profile.

1.3.5 Interfaces and Reference Points[1]

As already explained, the E-UTRAN is an all-IP network. Figure 1.10 shows the network elements that are typically involved in the signaling procedures and routing of payload data from the UE to the PDN and vice versa. The figure also shows the reference points for inter-RAT handover (and inter-RAT packet routing) between E-UTRAN, UTRAN, and GERAN.

The pipeline symbols in the figure illustrate the different signaling connections and tunnels for IP payload transport established and maintained during the connection. The signaling on Gx and Rx used to negotiate specific QoS policies is ignored for reasons of better understandability. Besides, the existence of the PCRF is optional. Due to the fact that the MME and the S-GW may also be combined into a single physical entity, the S11 interface is also optional. The lab test scenarios existing at the time of writing (spring 2010) all have separated physical entities for the MME and S-GW.

The signaling connection across the LTE-Uu interface is the RRC signaling connection, represented by a set of Signaling Radio Bearers (SRBs). The user plane tunnel across LTE-Uu is the radio bearer

[1] Reproduced with permission from © 3GPP™.

(see also Section 1.6 in this book). The other user plane tunnels are named after the appropriate reference points: namely, S1 bearer and S5 bearer. After the PDN-GW the connection is carried by the external bearer on SGi. S1AP signaling between the E-UTRAN and MME will be used to establish the tunnel on S1-U and GTP-C signaling will be used to create the tunnel on S5. On SGi we can see already plain IP traffic – pure payload, so to say.

The reference points shown in Figures 1.11–1.13 can be briefly described as follows:

- **S1-MME**: Reference point for the control plane protocol between the E-UTRAN and MME. This control plane protocol is the S1AP, which is quite similar to UTRAN RANAP. Indeed, in early drafts of LTE specs this protocol was called "E-RANAP."
- **S1-U**: Reference point between the E-UTRAN and S-GW for the per bearer user plane tunneling and inter-eNB path switching during handover. The protocol used at this reference point is the GPRS Tunneling Protocol for the User Plane (GTP-U).
- **S3**: This is the reference point between the MME and SGSN. The SGSN may serve UTRAN, GERAN, or both. On S3 we can see plain control plane information for user and bearer information exchange for inter-3GPP access network mobility (inter-RAT handover) in the idle and/or active state. If the connection was set up originally in the E-UTRAN and is handed over to UTRAN/GERAN the appropriate user plane streams are routed across the S4 reference point. What happens in the case of UTRAN/GERAN to E-UTRAN handover depends on whether S-GW also acts as the anchor for UTRAN/GERAN traffic. If this is true the user plane tunnel can be switched smoothly between S4 and S1-U during the handover. The protocol used at the S3 reference point is the GTP-C.

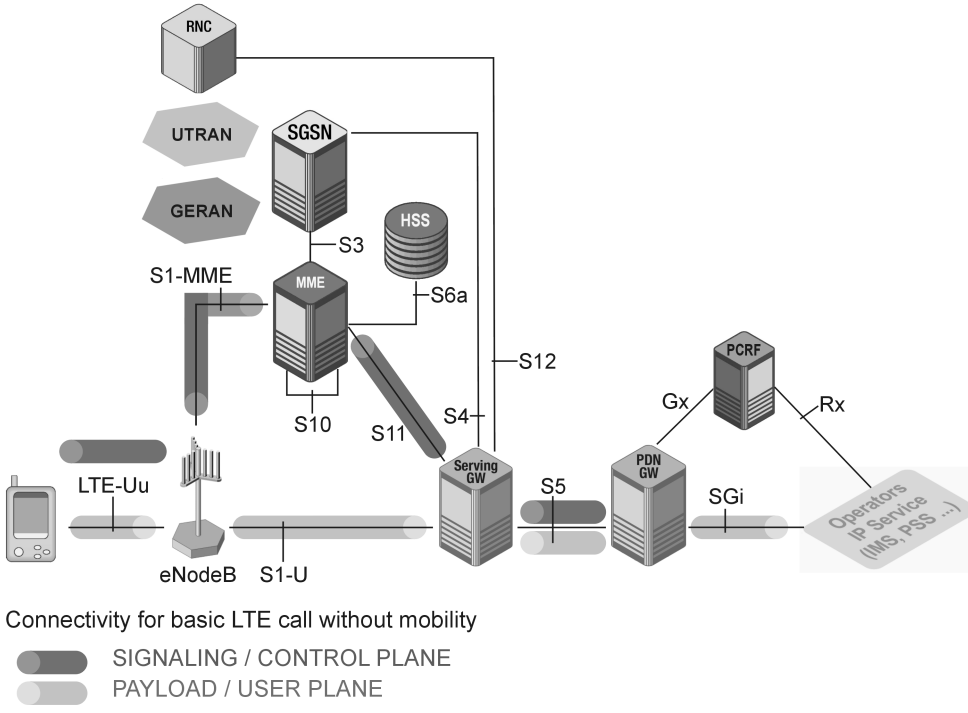


Figure 1.11 Connection via E-UTRAN non-roaming architecture.

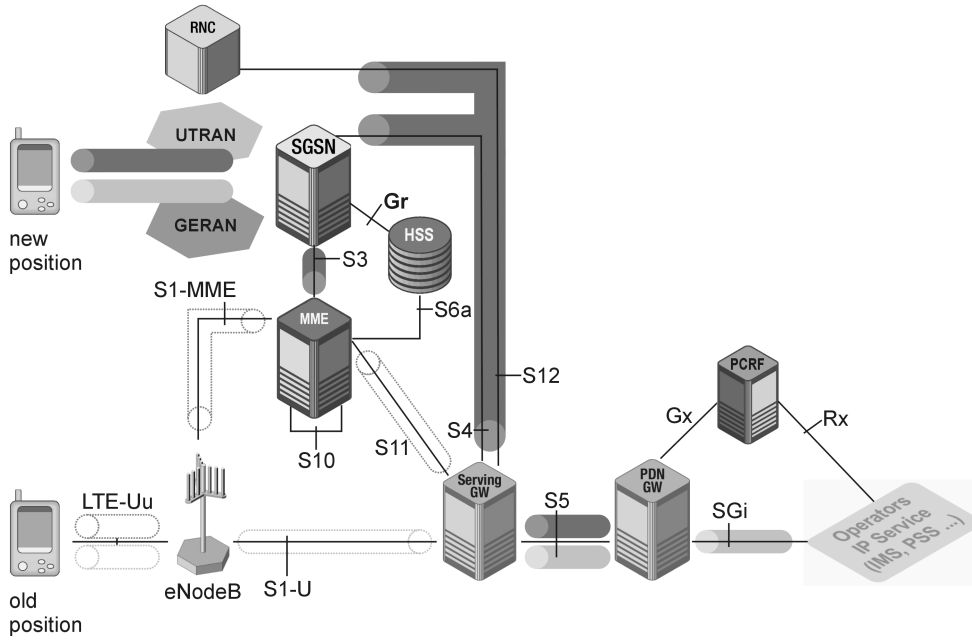


Figure 1.12 Connection after inter-RAT handover from E-UTRAN to UTRAN/GERAN.

- **S4**: The S4 reference point provides related control and mobility support between the GPRS core and the 3GPP anchor function of the S-GW using GTP-C. In addition, if a direct tunnel across S12 is not established, it provides user plane tunneling using GTP-U.
- **S5**: The S5 reference point provides user plane tunneling and tunnel management between the S-GW and PDN-GW. It is used in case of S-GW relocation due to UE mobility and if the S-GW needs to connect to a non-collocated PDN-GW for the required PDN connectivity. The protocol used at this reference point is GTP for both the control plane and user plane.
- **S6a**: The S6a reference point enables the transfer of subscription and authentication data for authorizing user access to the network. The reference point can be also described as the AAA interface between the MME and HSS. Compared to the legacy core network of 2G/3G standards, the functionality provided by S6a is similar to the one on the Gr interface, but due to the all-IP concept of EPC the protocol used at this reference point is the DIAMETER protocol. In the IP world DIAMETER is known as the successor of RADIUS, a protocol for granting access and authentication. However, the DIAMETER used on S6a does not have much in common with what is found in the IP world. The protocol header is based on IP standards, but the messages and parameters on the application layer are defined in a 3GPP-specific DIAMETER standard that has no meaning in the IP world.
- **Gx**: This point provides transfer of (QoS) policy and charging rules from the PCRF to the Policy and Charging Enforcement Function (PCEF) in the PDN-GW. This means that a set of rules for charging the transmission of a particular user data stream (called service flow) will be requested by the PDN-GW upon bearer establishment and the PCRF will provide the required parameters for the charging process. Especially, it will signal which of the following charging models will apply:
  - Volume-based charging.
  - Time-based charging.

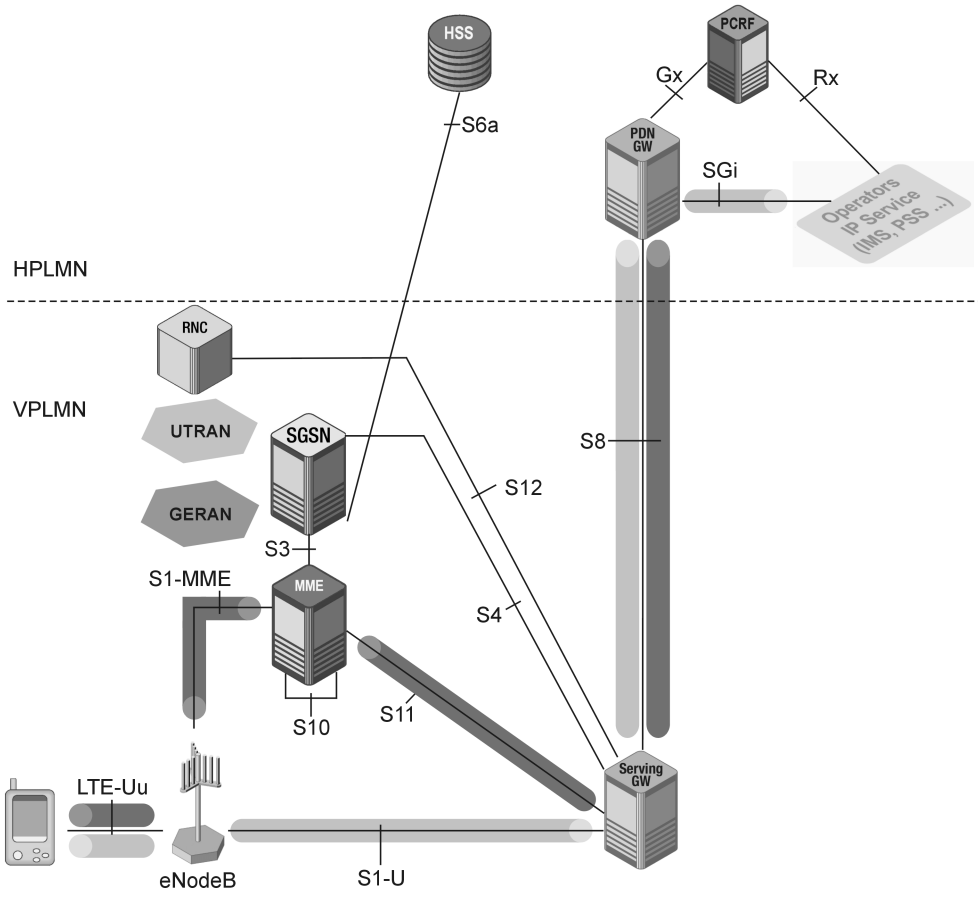


Figure 1.13 Connection via E-UTRAN with roaming in EPC.

  - Volume- and time-based charging.
  - Event-based charging.
  - No charging (if the user pays at a monthly flat rate).
    Also, information about prepaid limits and other thresholds can be included.
- **S8**: The S8 reference point is used by roaming subscribers only. It is the inter-PLMN reference point providing the user plane and control plane between the S-GW in the Visited PLMN (VPLMN) and the PDN-GW in the Home PLMN (HPLMN). S8 is the inter-PLMN variant of S5, based on GTP as well, and can be compared to the Gp interface defined for GERAN GPRS.
- **S8**: The S8 reference point is also used by roaming subscribers only. It provides transfer of (QoS) policy and charging control information between the home PCRF and the visited PCRF in order to support the local breakout function. For example, imagine a prepaid limit that can only be known by the home PCRF and must be provided to the visited PCRF to allow roaming services for this user.
- **S10**: This is the reference point between MMEs for MME relocation and MME-to-MME information transfer. This reference point provides mobility functions for intra-E-UTRAN handover/relocation. In other words, signaling procedures on this interface are triggered by UE mobility. It

should be noted that this kind of MME relocation in 3GPP 23.401 is called S1 handover. Hence, S10 is seen as special kind of S1 interface and the S1AP is used at this reference point.

- **S11**: This is the reference point between the MME and S-GW. The protocol used here is the GTP-C. The appropriate user plane is routed across S1-U.
- **S12**: The S12 reference point is located between the RNC in the 3G UTRAN and the S-GW for user plane tunneling when a "direct tunnel" is established. It is based on the Iu user plane and Gn user plane reference points using the GTP-U as defined between the SGSN and RNC, or between the SGSN and GGSN in the 3G core network. Use of the S12 reference point is an operator configuration option. On S12 only GTP-U traffic can be monitored, as on S1-U.
- **S13**: This point enables a UE identity check procedure between the MME and EIR (Equipment Identity Register). Typically there is no EIR installed in public networks due to the high administrative efforts, but this network element is found in some private networks. For instance, the GSM-based mobile network of the railway company Deutsche Bahn is equipped with an EIR. The purpose is to ensure that only staff of Deutsche Bahn can use the company's PLMN, but no private persons and staff of other European railway companies such as France's SNCF that also runs trains through Germany.
- **SGi**: This is the reference point between the PDN-GW and the packet data network. This network may be an operator external public or private packet data network or an intra-operator packet data network, for example for the provision of IP Multimedia Subsystem (IMS) services. To simplify the definition, it can be said that for many user plane connections SGi is the interface to the public Internet. This reference point corresponds to Gi for 3GPP access. Typically the complete TCP/IP suite can be monitored at this point.
- **Rx**: The Rx reference point resides between the Application Function (AF) and the PCRF defined in 3GPP 23.203. It is for instance mandatory if real-time communication services such as Voice over IP (VoIP) are to be charged differently than common PS data transfer.
- **SBc**: The SBc reference point lies between the Cell Broadcast Center (CBC) and MME for warning message delivery and control functions. This interface is used to broadcast warning messages to subscribers (not to send warning messages about network element status to the operation and maintenance center). A typical example of such warning messages could be the broadcast of bush fire or tsunami alarms.

The special anchor function of the S-GW can be illustrated when looking at a connection that was handed over from the E-UTRAN to UTRAN or GERAN as shown in Figure 1.12. In this case the connections on S5 and SGi remain the same, but the payload is now routed through a tunnel across S4 or S12 while the signaling necessary to execute the inter-RAT mobility will be sent across S3. The old bearers and signaling connections on S1 and LTE-Uu will be deleted after successful handover of the connection.

Figure 1.13 illustrates the basic connection of a roaming subscriber. Signaling and payload take the same route as in Figure 1.12, but the HSS and PDN-GW and, thus, the connection to the public packet network are located in a foreign network. The IP tunneling from the S-GW to PDN-GW and vice versa is realized through the S8 interface, which has identical protocol structure and functions to S5. The only difference is that S8 must fulfill higher requirements in terms of inter-operability, because equipment from different manufacturers must be interconnected through this reference point.

1.4 Area and Subscriber Identities

1.4.1 Domains and Strati

For the EPC a complete new NAS was designed including a new NAS protocol layer described in 3GPP 24.301.

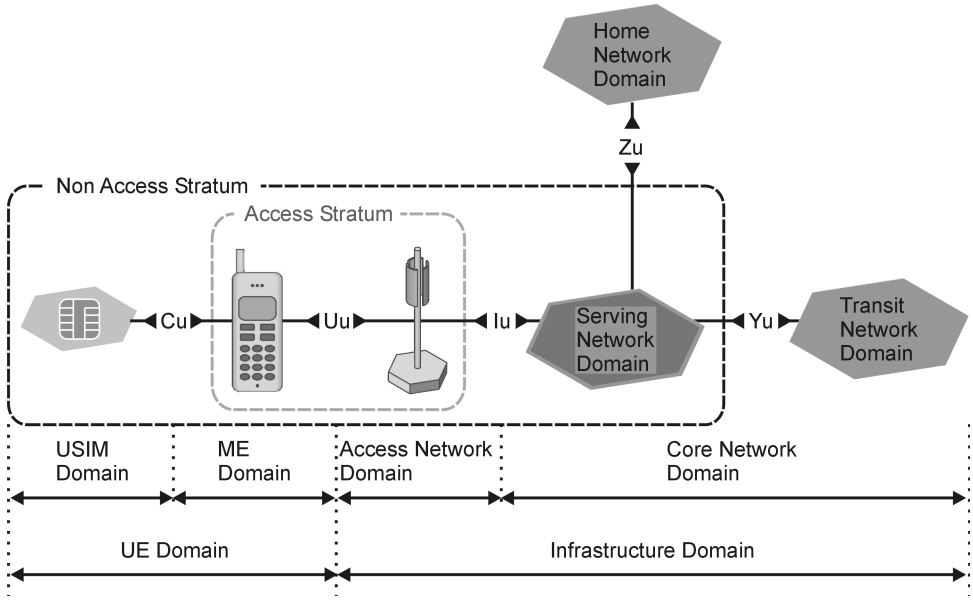


Figure 1.14 Domains and strati in E-UTRAN and EPC.

In contrast to the core network of 3GPP Release 99 to Release 6 where a CS and PS domain were defined as subdomains of the serving network domain, the EPC will not host any CS domain due to its all-IP character. However, it still distinguishes between AS and NAS signaling and functions as shown in Figure 1.14.

The AS comprises the radio chipset of the UE including the RRC protocol entity and all underlying transport layer entities. Here all parameters that more or less frequently change during radio access can be found, including transport formats and radio-specific identities of serving cell and possible handover candidates (neighbor cells).

The NAS covers all signaling exchanged between the USIM (UMTS Subscriber Identity Module) and the core network node, in case of LTE radio access: the MME. This is the home of all parameters that allow unambiguous identification of a subscriber or the handset hardware such as International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI). There are also temporary identities stored on the USIM card like Temporary Mobile Subscriber Identity (TMSI) and Globally Unique Temporary UE Identity (GUTI). From a protocol point of view the NAS is the home of network access, initial subscriber registration, and mobility management procedures. Due to the all-IP concept of LTE/EPC, a new NAS protocol was defined, namely 3GPP 24.301, while similar functions for 2G/3G networks are defined in the standard 3GPP 24.008. The E-UTRAN NAS protocol 3GPP 24.301 does not contain any functions for CS call control and SMS. In the early planning stages of the E-UTRAN it was assumed that all speech services via the E-UTRAN would use VoIP and the IMS architecture. As an alternative the CS fallback option (implemented in the S1AP protocol) was designed, but obviously this did not satisfy the need for reliable and cost-efficient CS services in the E-UTRAN. Hence, an initiative formed of operators and Network Equipment Manufacturers (NEMs) started to work on the Voice over LTE via Generic Access standards (VoLGA). VoLGA is beyond the scope of 3GPP. Its principle is to establish an IP connection between the UE and E-UTRAN and use the radio bearer for transparent forwarding of 3GPP 24.008 NAS signaling message and AMR

(Adaptive Multirate) voice packets across the logical Z1 interface. Instead, in the S-GW the RAB used for VoLGA is terminated in a special protocol converter and media gateway device, the VoLGA Access Network Controller (VANC), that is, the interconnecting point between the E-UTRAN/EPC and UTRAN/GERAN/Legacy Core Network.

1.4.2 IMSI

The IMSI allows unambiguous identification of a particular SIM or USIM card. The IMSI is composed of three parts (Figure 1.15):

- The Mobile Country Code (MCC), consisting of three digits. The MCC uniquely identifies the country of domicile of the mobile subscriber. MCC values are administrated and allocated by an international numbering plan.
- The Mobile Network Code (MNC), consisting of two or three digits for GSM/UMTS applications. The MNC identifies the home PLMN of the mobile subscriber. The length of the MNC (two or three digits) depends on the value of the MCC. A mixture of two- and three-digit MNC codes within a single MCC area is not recommended and is beyond the scope of this specification.
- The Mobile Subscriber Identification Number (MSIN), identifying the mobile subscriber within a PLMN. As a rule the first two or three digits of the MSIN reveal the identity of the Home Location Register (HLR) or HSS that is used for Signaling Connection Control Part (SCCP) Global Title translation procedures when roaming subscribers register in foreign networks.

The National Mobile Subscriber Identity (NMSI) consists of the MNC and the MSIN.

A combination of MCC and MNC can be used to aggregate call-specific performance measurement data (such as cumulative counters) on IMSI groups. This will help to highlight problems of roaming subscribers such as network failures during registration procedures, as described later in this book. Table 1.1 shows some samples from an IMSI group mapping table with MCC/MNC combinations in

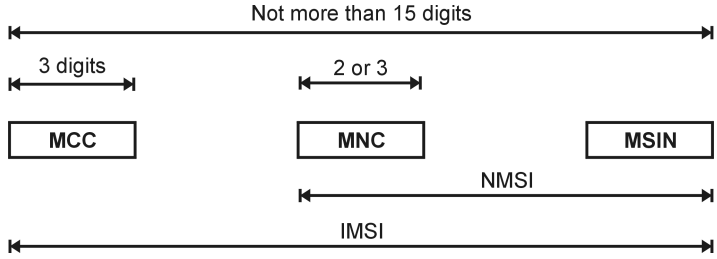


Figure 1.15 Structure of IMSI (according to 3GPP 23.303). Reproduced with permission from © 3GPP™.

Table 1.1 IMSI group mapping table from Tektronix Communications NSA software

<IMSI IMSINumber= '26201' IMSIGroupName= 'T-MOBILE DEUTSCHLAND GMBH (GERMANY)' />
<IMSI IMSINumber= '26202' IMSIGroupName= 'VODAFONE D2 GMBH (GERMANY)' />
<IMSI IMSINumber= '26801' IMSIGroupName= 'VODAFONE TELECEL (PORTUGAL)' />
<IMSI IMSINumber= '27201' IMSIGroupName= 'VODAFONE IRELAND PLC (IRELAND)' />
<IMSI IMSINumber= '310560' IMSIGroupName= 'T-MOBILE USA, INC. (UNITED STATES)' />

"IMSINumber" fields and operator names in the "IMSIGroupName" field. Note the three-digit MNC used for the American operator.

It is possible that one-use equipment will work with more than just one (U)SIM. A good example is a mobile phone that has both business and private SIM cards as one device. Depending on the nature of the call (private or business), the owner of the handset can choose which (U)SIM should be used to make the call. Such a procedure might be required in case private phone calls need to be charged separately due to national income tax laws (as found, for example, in Germany).

1.4.3 LMSI, TMSI, P-TMSI, M-TMSI, and S-TMSI

All temporary subscriber identities, Local Mobile Subscriber Identity (LMSI), TMSI, and P-TMSI, will not be seen in E-UTRAN signaling as long as there is no inter-RAT mobility between the E-UTRAN and UTRAN/GERAN. Indeed, for LTE a new NAS protocol was specified (3GPP 24.301) that introduces a new temporary subscriber identity for the E-UTRAN: the GUTI described in Section 1.4.4. However, to fulfill inter-RAT mobility requirements TMSI, P-TMSI, and LMSI will still be found in E-UTRAN NAS messages, or at least it will be indicated if valid values of these parameters are stored on the USIM card.

The LMSI is a four-octet/byte number. It is a pointer to a database record for a particular IMSI in the Visitor Location Register (VLR) database. Although the VLR is no longer found in the EPC network architecture, there is a database with the same function hosted by the MME. The purpose of the LMSI was to speed up the search for particular database records. If this is still required, with the new powerful computer hardware used to build today's network elements it is a design detail to be defined by NEMs. From definitions given in 3GPP 23.003 it can be guessed that the LMSI will not be used by the MME.

The TMSI is also encoded as a four-octet/byte hex number. It is allocated to a particular subscriber (more correctly, to a particular subscriber's (U)SIM card) during initial attach. The TMSI is used to mask the true subscriber's identity, which is the IMSI, in NAS signaling procedures. In the E-UTRAN it is often used together with the GUTI. It can be coded using a full hexadecimal representation. Since the TMSI has only local significance (i.e., within a VLR and the area controlled by a VLR, or within a SGSN and the area controlled by a SGSN, or within a MME and the area controlled by a MME), the structure and coding of it can be chosen by agreement between the operator and manufacturer in order to meet local needs.

The TMSI allocation procedure should always be executed in ciphered mode to prevent unauthorized eavesdropping.

The P-TMSI is the complement of TMSI in the UTRAN/GERAN PS domain. It is allocated by the SGSN and, hence, will be monitored in the EPC and E-UTRAN during inter-RAT handover/relocation preparation and execution. The P-TMSI is encoded in the same way as the TMSI. The difference is in defining value ranges. If the first two leading digits have the value "11" the parameter is identified as a P-TMSI. Thus, in the hexadecimal format, all TMSI values starting with C, D, E, or F as the first hex number are P-TMSIs.

The M-TMSI is a 32-digit binary number that is part of the GUTI and exclusively used in the E-UTRAN.

The S-TMSI consists of the Mobility Management Entity Code (MMEC) and M-TMSI. Indeed, it is just a shorter variant of the GUTI.

1.4.4 GUTI

The GUTI is assigned only by the MME during initial attach of a UE to the E-UTRAN.

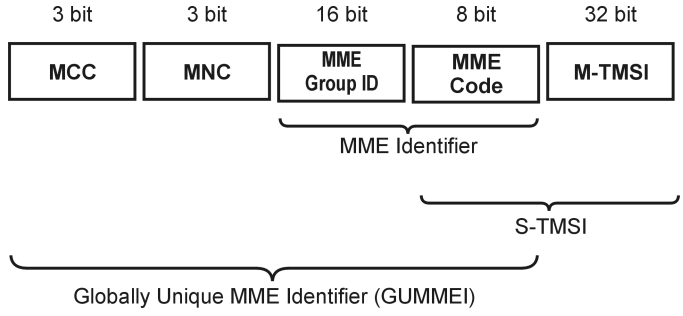


Figure 1.16 Format of GUTI and S-TMSI.

The purpose of the GUTI is to provide an unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the E-UTRAN. It also allows identification of the MME and network to which the UE attaches. The GUTI can be used by the network to identify each UE unambiguously during signaling connections.

The GUTI has two main components: the Globally Unique Mobility Management Entity Identifier (GUMMEI) that uniquely identifies the MME which allocated the GUTI; and the M-TMSI that uniquely identifies the UE within the MME that allocated the GUTI. The GUMMEI is constructed from the MCC, MNC, and Mobility Management Entity Identifier (MMEI).

The MMEI should be constructed from a Mobility Management Entity Group ID (MMEGI) and a MMEC. The GUTI should be constructed from the GUMMEI and the M-TMSI as shown in Figure 1.16.

For paging purposes, the mobile is paged with the S-TMSI. The S-TMSI is constructed from the MMEC and the M-TMSI. It is correct to say that the S-TMSI is a shorter format of GUTI that can be used because, after successful registration of a UE, the serving network as well as the serving MME group are known and stored in the core network databases.

The operator needs to ensure that the MMEC is unique within the MME pool area and, if overlapping pool areas are in use, unique within the area of overlapping MME pools.

The GUTI should be used to support subscriber identity confidentiality and, in the shortened S-TMSI form, to enable more efficient radio signaling procedures (e.g., paging and service request).

MCC and MNC should have the same field size as described for the IMSI.

The M-TMSI has a length of 32 bits, MMEGI is 16 bits in length, and MMEC 8 bits in length.

It is important to understand that on the S1 interface the IMSI is typically not seen, just like the GUTI. Exceptions are initial attach to the network when no old GUTI is stored on the USIM card or the true subscriber's identity is checked using NAS signaling, which regularly happens when roaming subscribers attach. Also, in the case of the paging procedure the IMSI might be seen.

For monitoring and network performance measurement the IMSI on S1 can only be revealed if the changing temporary identities are tracked with a quite sophisticated architecture. Full IMSI tracking can only be ensured by monitoring *all* S1 interfaces of an operator's E-UTRAN and ideally all S6a interfaces and storing the current GUTI/IMSI relations in a central point as stored in the HSS.

1.4.5 IMEI

The IMEI or IMEISV is used to unambiguously identify the hardware and (with IMSISV) software version of a mobile phone. The IMEISV that is expected to be used for all 4G and UEs consists of 16 bits as shown in Figure 1.17.

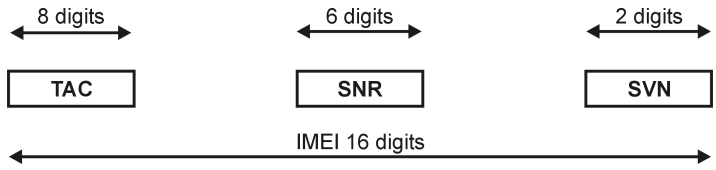


Figure 1.17 Structure of IMEISV (according to 3GPP 23.303). Reproduced with permission from © 3GPP™.

Table 1.2 Example of handset name mapping table

<Handset IMEI='35942100' HandsetName='MOTOROLA V3 RAZR' />
<Handset IMEI='35942200' HandsetName='MOTOROLA V3 RAZR' />
<Handset IMEI='35942300' HandsetName='MOTOROLA V3 RAZR' />
<Handset IMEI='01161200' HandsetName='APPLE IPHONE 3G' />
<Handset IMEI='01161300' HandsetName='APPLE IPHONE 3G' />
<Handset IMEI='01161400' HandsetName='APPLE IPHONE 3G' />
<Handset IMEI='35179700' HandsetName='SAMSUNG SGH-E100' />
<Handset IMEI='35179800' HandsetName='SAMSUNG SGH-E100' />
<Handset IMEI = '35179900' HandsetName = 'SAMSUNG SGH-A800' />

The eight leading digits stand for the Type Approval Code (TAC). This TAC indicates the manufacturer of the equipment. The next six digits stand for the Serial Number (SNR) and finally the two last digits represent the software version.

As shown in Table 1.2 (which gives a list for 3G handsets) the TAC (in the table named "Handset IMEI") is always unique for a particular equipment type, but due to large manufacturing series several TACs are assigned to the same type if the number of manufactured units exceeds the threshold of 100 000 that can be numbered with the six-digit SNR.

1.4.6 RNTI

In 3G UMTS the Radio Network Temporary Identifiers (RNTIs) are always used to identify information dedicated to a particular subscriber on the radio interface, especially if common or shared channels are used for data transmission. Now, in LTE it is the rule that common channels and shared channels are used to transmit all UE-specific data, but also some network-specific data across the radio interface. For this reason the RNTI in LTE is not always related to a particular subscriber, but sometimes also used to distinguish broadcast network information from data streams of subscribers.

The RNTI is signaled in the MAC layer.

When MAC uses the Physical Downlink Control Channel (PDCCH) to indicate radio resource allocation, the RNTI that is mapped on the PDCCH depends on the logical channel type:

- C-RNTI, Temporary Cell Radio Network Temporary Identifier (temp C-RNTI), and Semi-Persistent Scheduling (SPS) C-RNTI for Dedicated Control Channel (DCCH) and DTCH;
- Paging Radio Network Temporary Identity (P-RNTI) for Paging Control Channel (PCCH);
- Random Access Radio Network Temporary Identifier (RA-RNTI) for Random Access Response (RAR) on DL-SCH;
- Temporary C-RNTI for Common Control Channel (CCCH) during the random access procedure;
- System Information Radio Network Temporary Identifier (SI-RNTI) for Broadcast Control Channel (BCCH).

Table 1.3 RNTI values (according to 3GPP 36.321). Reproduced with permission from © 3GPP™

Value (hexadecimal)		RNTI
FDD	TDD	
0000-0009	0000-003B	RA-RNTI
000A-FFF2	003C-FFF2	C-RNTI, semi-persistent scheduling C-RNTI, temporary C-RNTI, TPC-PUCCH-RNTI, and TPC-PUSCH-RNTI
FFF3-FFFC		Reserved for future use
FFFE		P-RNTI
FFFF		SI-RNTI

All RNTIs are encoded using the same 16-bit format (two octets = 2 bytes).[2]
The following values (given in Table 1.3) are defined for the different types of RNTI.

1.4.6.1 P-RNTI

The P-RNTI is the 4G complement of the paging indicator known from 3G UMTS. It does not refer to a particular UE, but to a group of UEs.

The P-RNTI is derived from the IMSI of the subscriber to be paged and constructed by the eNB. For this reason the IMSI is transmitted in a S1AP paging message from the MME to eNB, although in other S1 signaling only the GUTI is used to mask the true identity of the subscriber.

1.4.6.2 RA-RNTI

The RA-RNTI is assigned by the eNB to a particular UE after this UE has sent a random access preamble on the Physical Random Access Channel (PRACH). If this random access preamble is received by the eNB and network access granted, the base station sends an acquisition indication back to the mobile and this acquisition indication message contains the RA-RNTI. In turn the UE will use the RA-RNTI to send a RRC connection request message on the radio interface UL and the parameter will help to distinguish messages sent by different UEs on the Random Access Channel (RACH).

1.4.6.3 C-RNTI

The C-RNTI is a 16-bit numeric value. Its format and encoding are specified in 3GPP 36.321 (MAC). The C-RNTI is part of the MAC Logical Channel Group ID field (LCG ID). It defines unambiguously which data sent in a DL direction within a particular LTE cell belongs to a particular subscriber. For instance, all RRC messages belonging to a single connection between a UE and the network are marked with the same C-RNTI value by the MAC entity that provided transport services to the RRC and NAS. Thus, C-RNTI is an important parameter for call tracing.

The C-RNTI comes in three different flavors: temp C-RNTI, semi-persistent scheduling C-RNTI, and permanent C-RNTI.

The temp C-RNTI is allocated to the UE during random access procedure (with a RRC connection setup message) and may turn into a permanent C-RNTI depending on the result of a subsequently performed contention resolution procedure or in the case of contention-free random access.

[2] The terms octet and byte have the same meaning, but the origin is different. While "octet" was used in the telecommunication standards of CCITT and ITU to describe a field of 8 bits, in computer science and hence in the TCP/IP standardization the term "byte" was introduced.

The semi-persistent scheduling C-RNTI is used if the subscriber is running services with a predictable unchanging QoS profile. A typical example is VoIP for which the required bit rate will not change during the entire connection. In such a case the dynamic (re)scheduling of radio resources, which is mandatory in the case of bursty payload traffic to ensure optimal usage of resource blocks, is not required. The SPS C-RNTI is used to indicate an area of resource blocks that will be used by the same UE for a longer time frame without any expected change.

1.4.6.4 SI-RNTI

The SI-RNTI is sent on the PDCCH. It does not stand for a particular UE identity. Instead it signals to all mobiles in a cell where the broadcast System Information Blocks (SIBs) are found on the Physical Downlink Shared Channel (PDSCH). This is necessary since the PDSCH is used to transport both broadcast system information for all UEs and signaling/payload for particular mobiles. In other words, the SI-RNTI indicates which DL resource blocks are used to carry SIBs that in 3G UMTS have been sent on the broadcast (transport) channel mapped onto the Primary Common Control Physical Channel (P-CCPCH). In LTE there is no CCPCH, only DL-SCH.

1.4.7 Location Area, Routing Area, Service Area, Tracking Area, Cell Global Identity

The Location Area (LA) and Routing Area (RA), known from 2G and 3G RAN, will be used in the E-UTRAN only if the UE was involved in inter-RAT mobility procedures.

The LA is a set of cells (defined by the mobile operator) throughout which a mobile that is camping on UTRAN or GERAN will be paged. The LA is identified by the Location Area Identity (LAI) within a PLMN. The LAI consists of the MCC, MNC, and Location Area Code (LAC) – see Figure 1.18.

The RA is defined as a sub-area of a LA with specific means for PS services. Each UE informs the SGSN about the current RA. RAs can consist of one or more cells. Each RA is identified by a Routing Area Identity (RAI). The RAI is used for paging and registration purposes and consists of the LAC and Routing Area Code (RAC). The RAC (length 1 octet, fixed) identifies a RA within a LA and is part of the RAI.

The RAI is composed of the following elements, shown in Figure 1.19:

$$<\text{MCC}><\text{MNC}><\text{LAC}><\text{RAC}>$$

The Tracking Area Identity (TAI) is the identity used to identify tracking areas. The TAI is constructed from the MCC, MNC, and TAC (Tracking Area Code).

A Tracking Area (TA) includes one or several E-UTRAN cells. Although the details of TA design are subject to individual radio network planning, it can be guessed that a TA will typically be defined as a single E-UTRAN cell or all cells of an eNB. In theory a single eNB or even a single cell may

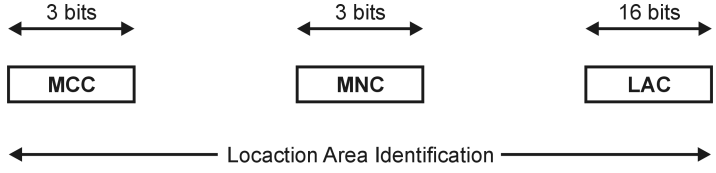


Figure 1.18 Structure of location area identification (according to 3GPP 23.303). Reproduced with permission from © 3GPP™.

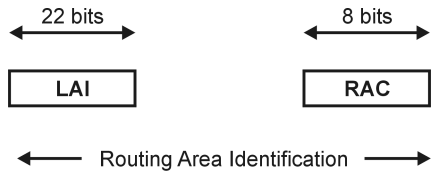


Figure 1.19 Structure of routing area identification (according to 3GPP 23.303). Reproduced with permission from © 3GPP™.

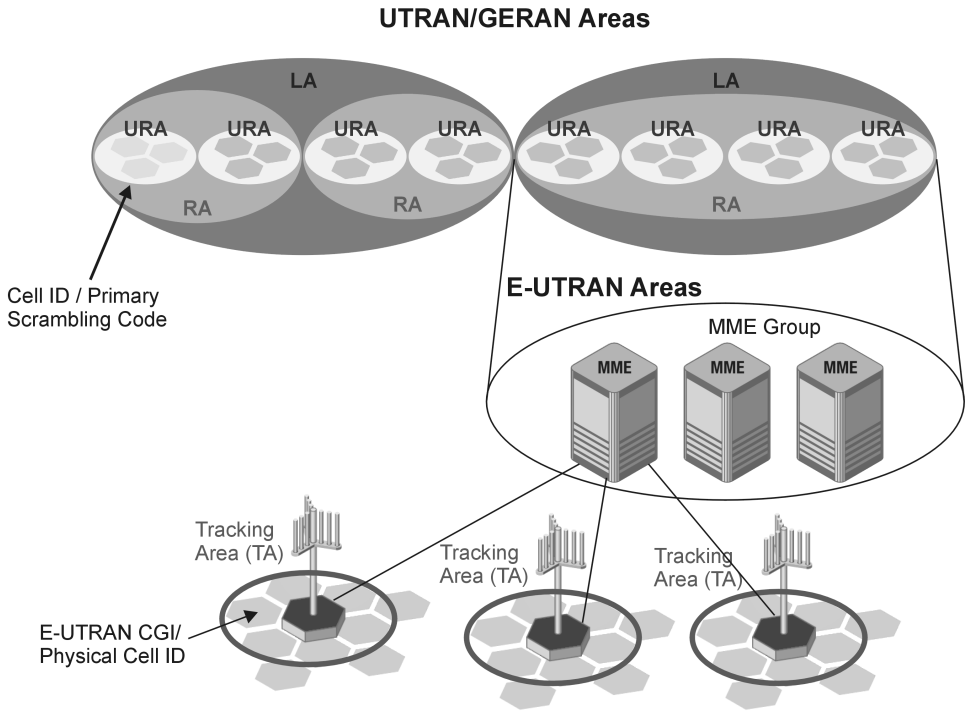


Figure 1.20 Areas in UTRAN/GERAN and E-UTRAN.

also belong to multiple TAs, for example, in the case of network sharing. In any case the details of area configuration are defined in radio network planning using proprietary definitions and rules. The scheme shown in Figure 1.20 is based on the assumption that in a typical network plan one TA covers all cells of one eNB.

A UTRAN/GERAN LA corresponds to a MME group as defined in 3GPP standards – see Section 1.4.8. Surely, each MME may also work as a MME group on its own.

The network allocates a list with one or more TAs to the UE. In certain operating modes, the UE may move freely in all TAs of the list without updating the MME.

The E-UTRAN Cell Global Identity (CGI) consists of the PLMN-ID (MCC + MNC) plus the E-UTRAN Cell Identity (CI), a 28-bit string. The leftmost bits of the CI correspond to the eNB ID. Using the E-UTRAN CGI, any cell in any E-UTRAN in the world can be unambiguously identified. To have a unique format for all cells in all RATs also for GERAN and UTRAN cells, a global CI is

defined; since Release 8 it is requested that these identities are broadcast in each cell and included in RRC measurement reports.

Indeed, on the radio interface the cells of the different RATs are identified by the following parameters:

- **GERAN**: Absolute Radio Frequency Channel Number (ARFCN) + Base Station Color Code (BCC).
- **UTRAN**: UMTS Absolute Radio Frequency Channel Number (uARFCN) + primary scrambling code.
- **E-UTRAN**: eARFCN + physical Cell ID (c-ID) (in fact also a scrambling code).

The ARFCN values are used to identify the frequency of the cell.

1.4.8 Mapping between Temporary and Area Identities for EUTRAN- and UTRAN/GERAN-Based Systems[3]

For the construction of the RA update request message in GERAN/UTRAN or TA update request message in E-UTRAN the following identities should be included.

In GERAN and UTRAN the RAI is constructed from the MCC, MNC, LAC, and RAC. In addition, the routing area update request message contains the P-TMSI that includes the mapped Network Resource Identifier (NRI) that is used in Iu flex networks. (An example of NRI usage is given in Kreher and Ruedebusch, 2007.)

P-TMSI should be of 32-bit length where the two topmost bits are reserved and always set to 11. These are needed since the GERAN representation of P-TMSI, of the form TLLI (Temporary Logical Link Identity), imposes this restriction. Hence, for a UE which may hand over to GERAN/UTRAN (based on subscription and UE capabilities), the corresponding bits in the M-TMSI are set to 11.

The NRI field is of variable length and should be mapped into the P-TMSI starting at bit 23 and down to bit 14. The most significant bit of the NRI is located at bit 23 of the P-TMSI regardless of the configured length of the NRI.

In the case of a combined MME-SGSN node, the NRI of the SGSN part and the MMEC of the MME part refer to the same combined node. The RAN configuration allows NAS messages on GERAN/UTRAN and E-UTRAN to be routed to the same combined node. The same or different values of NRI and MMEC may be used for a combined node.

The mapping of the GUTI should be done to a combination of the RAI of GERAN/UTRAN and the P-TMSI as follows:

E-UTRAN <MCC>	maps to GERAN/UTRAN <MCC>
E-UTRAN <MNC>	maps to GERAN/UTRAN <MNC>
E-UTRAN <MME Group ID>	maps to GERAN/UTRAN <LAC>
E-UTRAN <MME Code>	maps to GERAN/UTRAN <RAC>

It is also copied into the eight most significant bits of the NRI field within the P-TMSI.
E-UTRAN <S-TMSI> maps as follows:

- 22 bits of the E-UTRAN <M-TMSI> starting at bit 30 and down to bit 9 are mapped into the remaining 22 bits of the GERAN/UTRAN <P-TMSI>;
- the remaining 8 bits of the E-UTRAN <M-TMSI> are copied into 8 bits of the <P-TMSI signature> field.

[3] Reproduced with permission from © 3GPP™.

For the UTRAN, the 10-bit-long NRI bits are masked out from the P-TMSI and also supplied to the RAN node as an Intra-Domain NAS Node Selector (IDNNS).

The mapping of P-TMSI (TLLI) and RAI in GERAN/UTRAN to GUTI in E-UTRAN should be performed as follows:

GERAN/UTRAN <MCC>	maps to E-UTRAN <MCC>
GERAN/UTRAN <MNC>	maps to E-UTRAN <MNC>
GERAN/UTRAN <LAC>	maps to E-UTRAN <MME Group ID>
GERAN/UTRAN <RAC>	maps to 8 bits of the M-TMSI

The eight most significant bits of GERAN/UTRAN <NRI> map to the MMEC.

GERAN/UTRAN <P-TMSI or TLLI> excluding the eight most significant bits at the NRI position maps to the remaining bits of the M-TMSI.

The values of <LAC> and <MME group id> should be disjoint, so that they can be differentiated. It is recommended that the most significant bit of the <LAC> be set to zero, and the most significant bit of <MME group id> set to one.

1.4.9 GSM Base Station Identification[4]

To identify the target cell of an inter-RAT handover from the E-UTRAN to GERAN and possible handover candidates in RRC measurement reports, it is necessary to know how these cells are identified on the radio interface and in core network signaling procedures.

1.4.9.1 CI and CGI

The BSS and cell within the BSS are identified within a LA or RA by adding a CI to the LA or RA identification, as shown in Figure 1.21. The CI is of fixed length with two octets and can be coded using a full hexadecimal representation.

The CGI is the concatenation of the LA identification and the CI. The CI should be unique within a LA.

1.4.9.2 Base Station Identity Code (BSIC)

The BSIC is a local color code that allows a MS to distinguish between different neighboring base stations. The BSIC is a 6-bit code which is structured as shown in Figure 1.22.

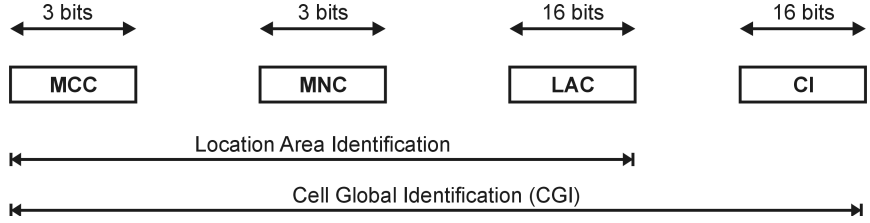


Figure 1.21 Structure of cell global identification (according to 3GPP 23.303). Reproduced with permission from © 3GPP™.

[4] Reproduced with permission from © 3GPP™.

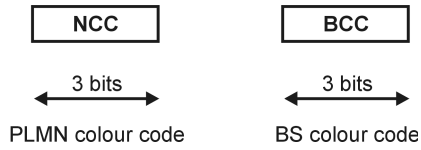


Figure 1.22 Structure of BSIC (according to 3GPP 23.303). Reproduced with permission from © 3GPP™.

In the definition of the Network Color Code (NCC), care should be taken to ensure that the same NCC is not used in adjacent PLMNs which may use the same BCCH carrier frequencies in neighboring areas.

Imagine a border area between different countries such as Germany, Poland, and the Czech Republic where, in this area, the radio signals of different international mobile carriers overlap. Now, the NCC is used to distinguish between cells of the German, Polish, and Czech network operators that may operate on the same frequency (BCCH carrier) while the BCC is used to identify cells of different German carriers (e.g., Vodafone and T-Mobile) from each other.

1.4.10 UTRA Base Station Identification

The 3G Universal Terrestrial Radio Access (UTRA) cells are identified on the radio interface unambiguously by a combination of uARFCN and primary scrambling code.

In signaling procedures between network elements the NBAP c-ID is unambiguous within a single Radio Network Subsystem (RNS), which means an area controlled by a single RNC. The same NBAP c-ID might be reused by network architects in different RNC areas.

In signaling communication between RNCs (e.g., to prepare handover/relocation of subscribers) and toward core network elements, the Service Area Identity (SAI) is commonly used.

1.4.10.1 uARFCN and Primary/Secondary Scrambling Codes

In RRC measurement reports and RRC handover messages the primary scrambling code together with the uARFCN will be used to identify target cells for handover to the UTRAN and possible handover to UTRAN candidates.

The primary scrambling codes are integer values in the range 0–511. Radio network planners must ensure that cells with the same primary scrambling code and same uARFCN never overlap.

1.4.10.2 SAI

The SAI is constructed as follows:

$$<\text{MCC}><\text{MNC}><\text{LAC}><\text{SAC}>$$

It is encountered during initial NAS signaling transport from the RNC to core network elements and might be later updated according to changes in the best cell of an active set using the RANAP update location procedure. The SAI is also used a source and/or target ID for 3G–3G and 3G–2G relocation/handover procedures.

A Service Area Code (SAC) is often used to identify a single UTRAN cell. However, the authors have also seen configurations where one SAC is used to identify a particular antenna sector (area covered by one antenna) that is covered by two different UMTS frequencies. In this scenario the SAC

addressed two cells that used the same primary scrambling code but different uARFCN and different NBAP c-ID.

1.4.10.3 Shared Network Area Identifier

The Shared Network Area Identifier (SNA-ID) is a new identity introduced in Release 8 standards and used to identify an area consisting of one or more LAs. Such an area can be used to grant access rights to parts of a shared network to a UE in connected mode.

The SNA-ID consists of the PLMN-Id followed by the Shared Network Area Code (SNAC)

$$<\text{MCC}><\text{MCN}><\text{SNAC}>$$

where the SNAC is defined by the operator.

1.4.11 Numbering, Addressing, and Identification in the Session Initiation Protocol

The Session Initiation Protocol (SIP) addresses so-called Uniform Resource Identifiers (URIs). The generic format is defined as follows:

$$sip{:}user{:}password@host{:}port{:}uri\text{-}parameters?headers.$$

This format can be compared to the structure of an e-mail address (e.g., ralf@tektronix.com). Optionally some specific SIP parameters may be included in the SIP address. Among such parameters, it can be defined which transport protocol should be used to exchange SIP messages, for instance. Also, a priority can be given to messages, authentication procedures can be invoked, errors reported, and routing instructions given by using the header fields. Some header fields only make sense in requests or responses. These are called request header fields and response header fields, respectively. A complete list of header fields and their relation to different SIP methods can be found in RFC (Request For Comments) 3261.

At the end a SIP address monitored in a live network may look like this:

$$sip{:}ralf@tektronix.com;transport{=}tcp?priority{=}urgent.$$

Besides the recipient's name and host, this address contains a URI parameter to request transport of this SIP information using the reliable TCP, and the header information indicates that this SIP information will be treated with urgent priority.

1.4.12 Access Point Name

In the GPRS backbone, an Access Point Name (APN) is a reference to a GGSN. To support inter-PLMN roaming, the internal GPRS DNS (Domain Name System) functionality is used to translate the APN into the IP address of the GGSN.

In the EPC network the APN is found in GTP-C signaling when packet contexts are established, but it is no longer found in LTE NAS signaling. This means in turn that for 2.5G and 3G phones the APN is an important parameter to be stored on the (U)SIM card, but for 4G phones the APN does not need to be configured by the end user. This will also resolve the problem where many PDP context setup failures seen currently in the GERAN and UTRAN are due to an unknown or missing APN.

The APN is composed of two parts as follows:

- The APN network identifier; this defines to which external network the GGSN is connected and optionally a requested service by the MS. This part of the APN is mandatory.
- The APN operator identifier; this defines in which PLMN GPRS backbone the GGSN is located. This part of the APN is optional.

The APN operator identifier is placed after the APN network identifier. An APN consisting of both the network identifier and operator identifier corresponds to the DNS name of a GGSN; the APN has, after encoding as defined below, a maximum length of 100 octets.

The encoding of the APN follows the name syntax defined in RFC 2181 [18], RFC 1035 [19], and RFC 1123 [20]. The APN consists of one or more labels. Each label is coded as a one-octet length field followed by that number of octets coded as 8-bit ASCII characters. Following RFC 1035 [19], the labels should consist only of the alphabetic characters (A–Z and a–z), digits (0–9), and the hyphen (-). Following RFC 1123 [20], the labels should begin and end with either an alphabetic character or a digit. The case of alphabetic characters is not significant. The APN is not terminated by a length byte of zero.

Typical APNs are:

- mms.tim.net;
- wap.eplus.net;
- wap.beeline.ru;
- wap.debitel.de;
- web.vodafone.de;
- internet.t-mobile.

The APN of a 3G subscriber is stored in the USIM. In LTE NAS signaling the APN is no longer used, because it is chosen by the intelligent packet routing functions of MME. However, the APN Average Maximum Bit Rate (APN-AMBR) may be signaled to the UE by the MME to control the amount and bandwidth of UL traffic.

1.5 User Equipment

As in UMTS, the LTE mobile station is called User Equipment (UE). It is constructed using a modular architecture that consists of three main components (see Figure 1.23):

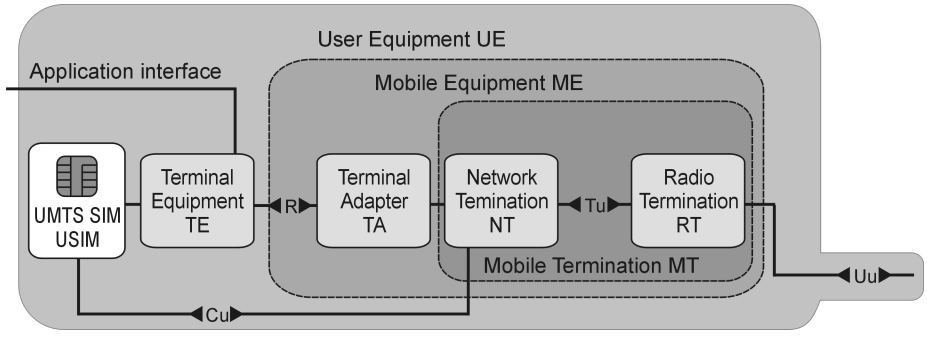


Figure 1.23 Modular architecture of a UE.

- **Mobile Termination**: The MT represents termination of the radio interface. In this entity the RRC signaling is terminated and RRC messages are sent/received.
- **Terminal Adapter**: The terminal adapter represents the termination of the application-specific service protocols, for example, SIP signaling for VoIP. The terminal adapter might be constructed as an external interface, for example, USB to connect a laptop PC using LTE technology with a mobile network.
- **Terminal Equipment**: The TE represents termination of the service. Depending on the UE's application capabilities, it may act as the TE or not. For instance, the Apple iPhone with its browser functionalities has full TE capability while a simple USB stick for mobile data transmission has no TE capability at all. In the case of the USB stick, the connected laptop PC is the TE.

1.5.1 UE Categories

The UE categories stand for an abstract grouping of common UE radio access capabilities and are defined in 3GPP 36.306.

In particular, the handset-type groups vary in maximum possible throughput (the maximum number of DL-SCH transport blocks bits received within a Time Transmission Interval (TTI)). Assuming a TTI of 1 ms for category 1, the maximum possible throughput is 10 296 bits/1 ms which is approximately 10 Mbps of physical layer DL throughput (including the RLC/MAC header information – so the payload throughput will be slightly less).

Category 5 mobiles are the only handsets that support 64 Quadrature Amplitude Modulation (QAM) on the UL as highlighted in Tables 1.4 and 1.5. The maximum possible bit rate ranges from 5 Mbps (Cat. 1) to 75 Mbps (Cat. 5).

1.6 QoS Architecture

The EPS bearer service layered architecture is depicted in Figure 1.24. Besides the different names of bearers and reference points, this architecture does not look very different from the bearer service architecture defined in Release 99. However, there is a major difference that is not obvious at first sight.

In 3G UMTS the request of a subscriber for a defined QoS of an end-to-end service starts the QoS negotiation procedure. This depends on the subscriber's subscribed QoS stored in the HLR and the available network resources which QoS is granted to a particular connection at the end. The QoS negotiation and control process starts on the NAS layer with the first SM message sent by the UE.

In LTE – different to 2.5 and 3G PS connections – a default bearer with a default QoS is already established when the UE attaches to the network. The QoS attributes of this default bearer

Table 1.4 UE categories and DL capabilities (according to 3GPP 36.306). Reproduced with permission from © 3GPP™

UE category	Maximum number of DL-SCH transport block bits received within a TTI	Maximum number of bits of a DL-SCH transport block received within a TTI	Approximate maximum bit rate DL (Mbps)
Category 1	10 296	10 296	10
Category 2	51 024	51 024	50
Category 3	102 048	75 376	75
Category 4	150 752	75 376	75
Category 5	302 752	151 376	150

Table 1.5 UE categories and UL capabilities (according to 3GPP 36.306). Reproduced with permission from © 3GPP™

UE category	Maximum number of bits of an UL-SCH transport block transmitted within a TTI	Support for 64QAM in UL	Approximate maximum bit rate UL (Mbps)
Category 1	5 160	No	5
Category 2	25 456	No	25
Category 3	51 024	No	50
Category 4	51 024	No	50
Category 5	75 376	Yes	75

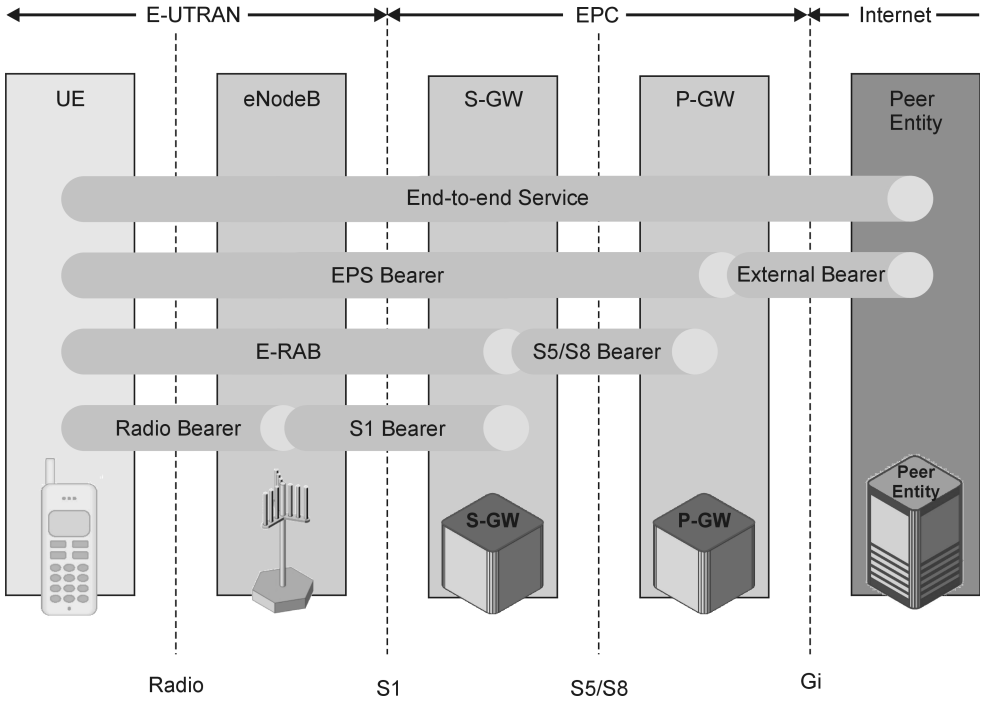


Figure 1.24 LTE QoS architecture (according to 3GPP 23.401). Reproduced with permission from © 3GPP™.

are determined by the subscribed QoS parameters stored in the HSS. This is still as seen in 2.5/3G networks.

However, if now the first user plane packet is sent by the UE it is routed toward the PDN where the PCRF analyzes the requested end-to-end service. Depending on this service, the PCRF may now trigger a modification of QoS parameters in all the involved bearers. There is no option for the subscriber to request a particular QoS; only the network is in charge of QoS control. There is also no way for the UE to request something known as a secondary context in 3G (see Section 3.26 in Kreher and Ruedebusch, 2007). In LTE all QoS management is tied to the application, not to SM signaling.

Ex.1013.00043

Table 1.6 Standardized QCI, QoS parameter thresholds, and example services (according to 3GPP 23.203). Reproduced with permission from © 3GPP™

QCI	Resource type	Priority	Packet delay budget (ms)	Packet error loss rate	Example services
1	GBR	2	100	10^{-2}	Conversational voice
2		4	150	10^{-3}	Conversational video (live streaming)
3		3	50	10^{-3}	Real-time gaming
4		5	300	10^{-6}	Non-conversational video (buffered streaming)
5	Non-GBR	1	100	10^{-6}	IMS signaling
6		6	300	10^{-6}	Video (buffered streaming) TCP based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100	10^{-3}	Voice, video (live streaming) interactive gaming
8		8	300	10^{-6}	Video (buffered streaming) TCP based
9		9			(e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)

It is important to understand that one UE in LTE can have multiple end-to-end services active and each of these services will have its own individual bearer. It is not intended by LTE standards that, for example, non-real-time services like web-browsing and e-mail will be mapped onto the same bearer (e.g., the same S1-U GTP tunnel) as we have seen in 3G UMTS. For this reason also 256 individual E-RABs for a single UE can be addressed by E-UTRAN protocols while in UMTS only 15 different RAB-IDs had been defined by the standard organizations.

In the 3GPP specs there is also a Traffic Flow Template (TFT) mentioned for the UL as well as for the DL part of the connection. These TFTs are bound to the EPS bearers. In general, a TFT can be described as a set of filters for a particular end-to-end service. Each TFT consists of a destination IP address and a set of source/destination port numbers. On the DL, the IP address is the address assigned to the UE; on the UL, it is the address of a server on the PDN. If we assume, for example, an HTTP 1.1 end-to-end service, the DL TFT of this service consists of the UE's IP address, the TCP source port number is 80, and the TCP destination port number is 80. On the UL, the port numbers are the same, but the IP address is the address of the server that hosts the web site.

To standardize the QoS handling, a set of nine QCIs have been defined by 3GPP. There are four classes with a Guaranteed Bit Rate (GBR) and five classes with a Non-Guaranteed Bit Rate (Non-GBR).

Besides the bit rate, the parameter priority, packet delay budget, and packet error loss rate are critical factors as given in Table 1.6.

1.7 LTE Security[5]

What are the new security functions in the E-UTRAN? This question can briefly be answered as follows.

[5] Reproduced with permission from © 3GPP™.

The first feature we see is a completely new ciphering mechanism and integrity protection for NAS signaling messages that was never seen in any 2G or 3G radio access network. On the radio interface this new NAS security leads to situations with double ciphering. On top of the protocol stack the NAS messages exchanged between the UE and MME are encrypted and the underlying RRC that acts as the transport layer for NAS is secured by ciphering mechanisms as well, so that the ciphered NAS message is ciphered together with its RRC transport message a second time.

The second new security feature is the option to secure the complete IP-based transport of the control plane and user plane on the S1 reference point using Secure IP (IPsec). There is no way to decipher IPsec by just monitoring the data that is exchanged between two endpoints of an IPsec connection. To decipher IPsec requires the monitoring software to be informed about which IPsec ciphering parameters (which can be changed frequently) are currently used in each of the involved endpoints of the IP connection. In a typical case these endpoints are the eNB and the MME or S-GW. To allow deciphering, there must be a dedicated Application Programming Interface (API) installed that allows the monitoring software to access IPsec-relevant parameters for deciphering. To design such an API requires close cooperation between the NEMs of eNB and MME/S-GW and the manufacturers of the monitoring software. The conclusion related to this fact is that free-of-charge monitoring software like WireShark will not be able to decipher IPsec. However, to obtain statistics of S1 control plane and user plane performance it is crucial to have metrics for E-UTRAN QoS and QoE (Quality of Experience). Consequently, IPsec deciphering will become one of the key differentiators for E-UTRAN monitoring software.

Besides these new security features, all the security elements from previous standards such as mutual authentication and masking of subscriber identity by using temporary identities can be found in the E-UTRAN. There is only a minor change here: the TMSI will be replaced by the new GUTI parameter.

To understand how the overall LTE security concept works, it is crucial to understand the hierarchy of LTE security keys first. This LTE security key hierarchy, shown in Figure 1.25, includes the following keys: K_{eNB}, K_{NASint}, K_{NASenc}, K_{UPenc}, K_{RRCint}, and K_{RRCenc}:

- **K_{eNB}** is a key derived by the UE and MME from K_{ASME} or by the UE and target eNB from Ke_{NB*} during eNB handover. K_{eNB} should only be used for the derivation of keys for RRC traffic and the derivation of keys for UP (User Plane) traffic, or to derive a transition key $K_{eNB}*$ during an eNB handover.

Keys for NAS traffic:

- **K_{NASint}** is a key which should only be used for the protection of NAS traffic with a particular integrity algorithm. This key is derived by the UE and MME from K_{ASME}, as well as an identifier for the integrity algorithm.
- **K_{NASenc}** is a key which should only be used for the protection of NAS traffic with a particular encryption algorithm. This key is derived by the UE and MME from K_{ASME}, as well as an identifier for the encryption algorithm.

Keys for UP traffic:

- **K_{UPenc}** is a key which should only be used for the protection of UP traffic with a particular encryption algorithm. This key is derived by the UE and eNB from K_{eNB}, as well as an identifier for the encryption algorithm.

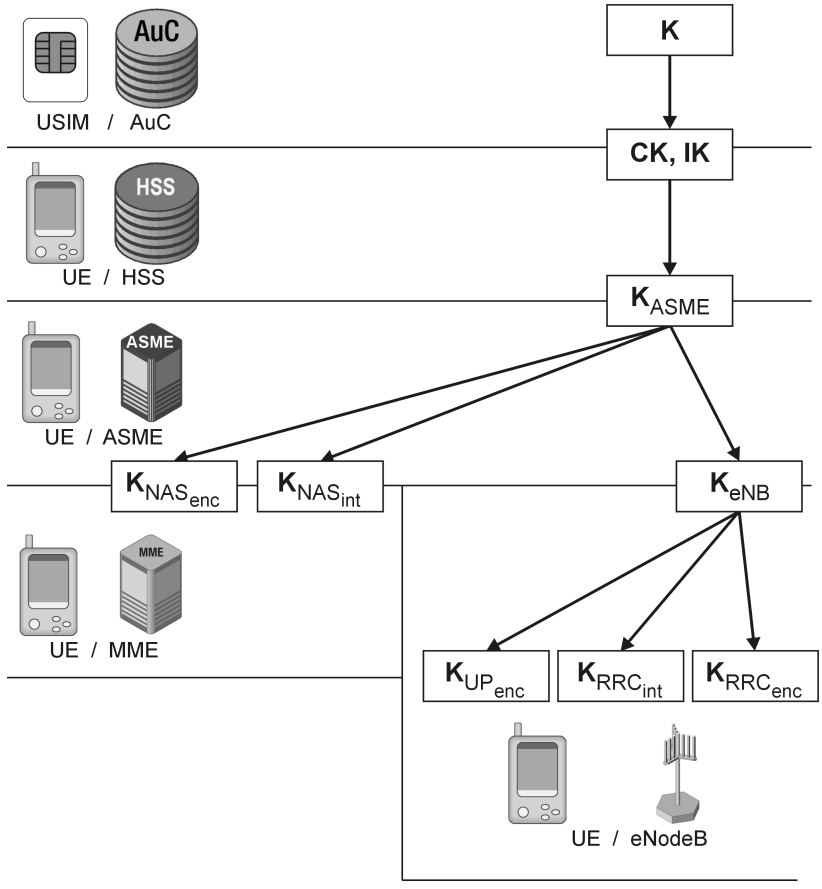


Figure 1.25 LTE security key hierarchy (according to 3GPP 33.401). Reproduced with permission from © 3GPP™.

Keys for RRC traffic:

- **K_{RRCint}** is a key which should only be used for the protection of RRC traffic with a particular integrity algorithm. K_{RRCint} is derived by the UE and eNB from K_{eNB}, as well as an identifier for the integrity algorithm.
- **K_{RRCenc}** is a key which should only be used for the protection of RRC traffic with a particular encryption algorithm. K_{RRCenc} is derived by the UE and eNB from K_{eNB} as well as an identifier for the encryption algorithm.

Now, whenever a call is established the security functions will work as shown in Figures 1.26–1.28. The start trigger of the security functions is when an initial NAS signaling message sent by the UE that contains UE security capability information arrives at the MME. The security capability list informs the MME for instance about which ciphering and integrity protection algorithms are supported by this UE.

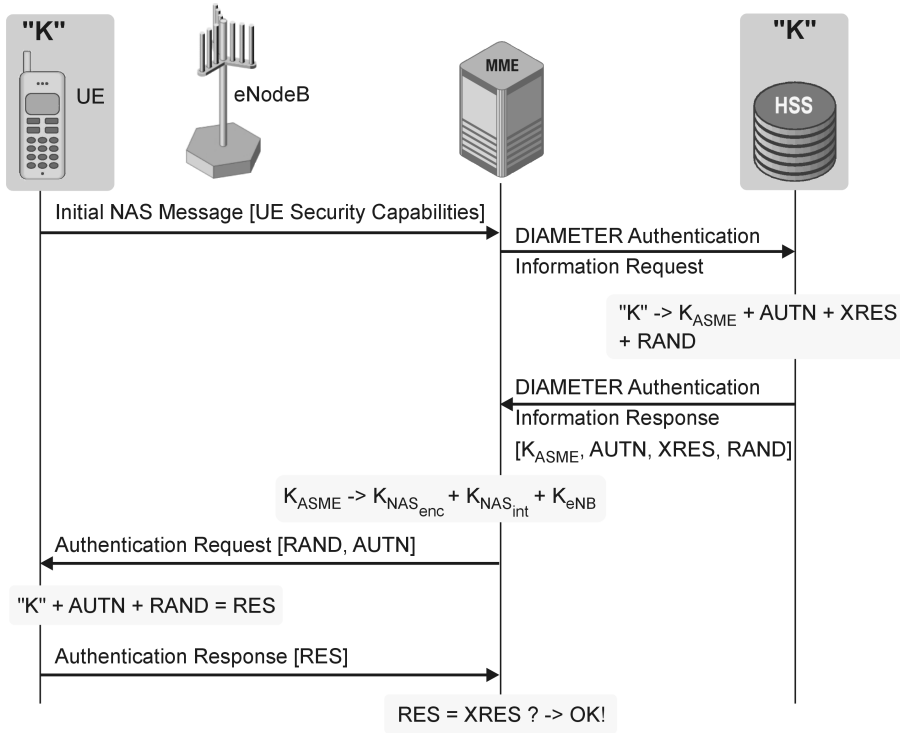


Figure 1.26 Subscriber authentication.

After the MME has received the initial NAS message and it has not been in contact with this subscriber before, or if all previously received security tokens sent by the HSS have been used, the MME must contact the HSS to receive new tokens. Thus, the MME sends a DIAMETER authentication information request message to the HSS that contains the subscriber's identity. The HSS holds the secret network key "K" that is also stored on the USIM card of each subscriber. "K" is unique to every network operator.

From "K" and the subscriber's identity the HSS derives three of the four parameters found inside the DIAMETER authentication information response message: the security key K_{ASME}, the Authentication Token (AUTN), and the Expected Response (XRES) parameter. The random number parameter RAND is truly just a random number.

After the MME has received these four parameters, it produces three more derivatives from K_{ASME}. These derivatives are the NAS encryption key K_{NASenc}, the NAS integrity protection key K_{NASint}, and the security key for the eNB K_{eNB}.

What follows is the authentication procedure between the MME and the UE. The MME sends the unciphered NAS authentication request message that includes the random number RAND and the AUTN. Now the UE must use its secret key "K" from the USIM card to calculate another number based on "K," AUTN, and RAND. The number is the UE's authentication response number RES.

RES is sent back to the MME by using the authentication response message, and in the last step of the authentication procedure the MME compares the value of RES to the value of XRES, which is the XRES value computed previously by the HSS. If RES and XRES have the same value the UE has successfully authenticated itself to the network and the NAS signaling connection can proceed.

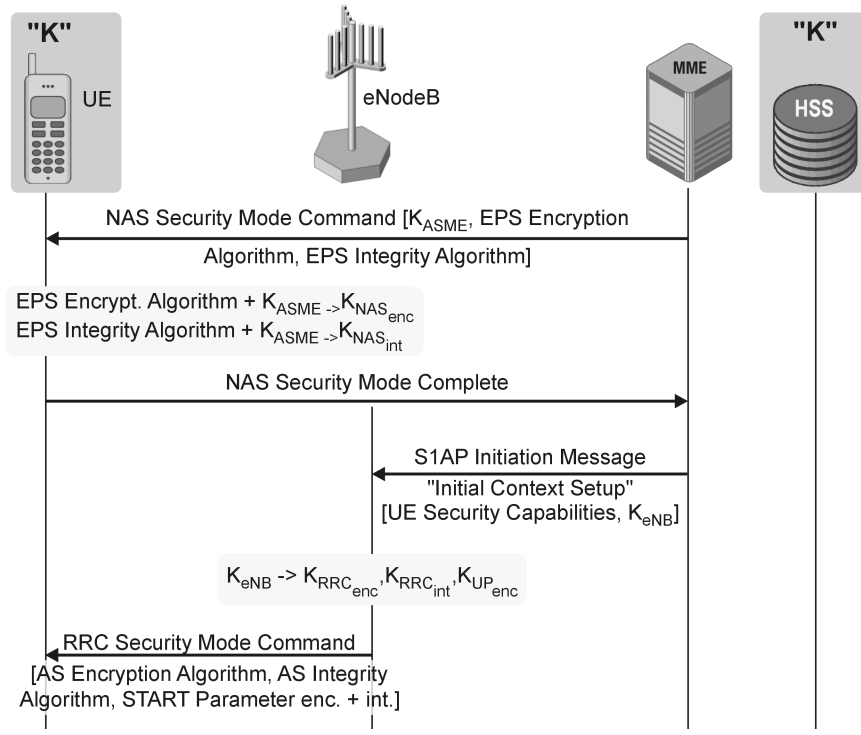


Figure 1.27 NAS security initiation and RRC security initiation.

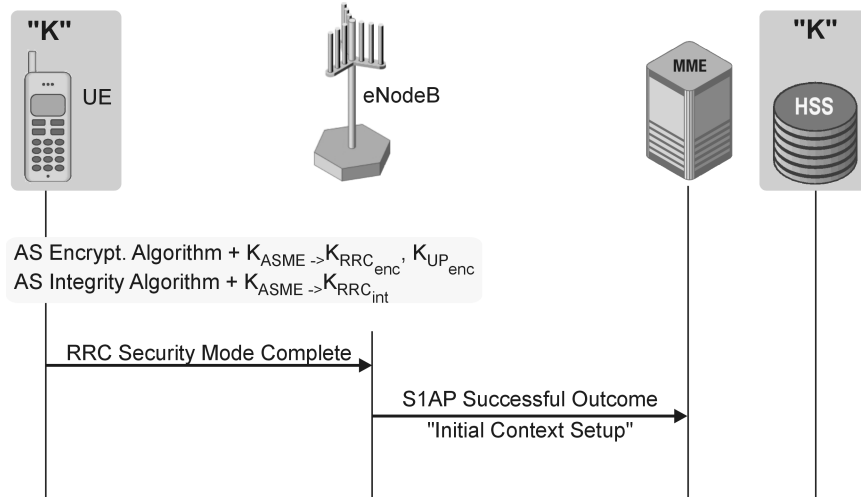


Figure 1.28 RRC security completion.

At this point, after successful authentication, it is time to activate the NAS security functions: namely, NAS ciphering and NAS integrity protection. Thus, the MME sends the NAS security mode command message to the UE including the security key K_{ASME} received previously from the HSS, and the algorithms for EPS encryption and EPS integrity protection that have been selected from the UE capability list and will be used to secure this NAS signaling connection.

After the UE has received the NAS security command, it computes on behalf of the assigned EPS encryption/integrity algorithms and the K_{ASME} key the keys for NAS encryption and NAS integrity protection that are identical to those already stored in the MME. Now NAS security is in service the UE sends back the NAS security mode complete message, which is the encrypted and integrity protected NAS message. It is not mandatory to use NAS encryption and integrity protection. It is always up to the operator to decide what is required to secure the network.

After the NAS security functions are in service, the underlying RRC connection and the ciphering for user plane traffic need to be activated. For this purpose, first a so-called security context is installed between the MME and eNB. Since security is not the only context-related information to be exchanged between these two network elements, the S1AP initial context setup message will also contain other parameters besides the UE security capabilities and the eNB's security key K_{eNB}. Note that the UE security capabilities so far are unknown to the eNB.

Now the eNB derives the keys for RRC encryption (K_{RRCenc}), RRC integrity protection (K_{RRCint}), and user plane encryption (K_{UPenc}) from K_{ASME}. Then the eNB sends the RRC security mode command message to the UE. This message contains the AS encryption algorithm and AS integrity protection algorithm bundled with the START parameters for the AS security activation procedure.

The UE computes the keys for RRC encryption (K_{RRCenc}), RRC integrity protection (K_{RRCint}), and user plane encryption (K_{UPenc}) from the K_{ASME} together with the received keys and activates the requested security functions using these parameters. After successful activation, the UE sends the RRC security mode complete message (i.e., ciphered and/or integrity protected) back to the eNB. And the eNB confirms the successful establishment of the security context to the MME by sending the S1AP successful outcome message for the procedure code "Initial Context Setup."

1.8 Radio Interface Basics

Wireless transmissions within mobile networks make use of electromagnetic waves to carry the transmitted information from source to destination. The data is modulated to complex waves (in a mathematical sense) using a modulation scheme. Furthermore, a duplex method (see Section 1.8.1) and a multiple access scheme or multiplex scheme (see Section 1.8.2) are applied to those complex waves. The resulting modulated spectrum is called baseband. The baseband carries all information and the utilized bandwidth of this baseband depends on the amount of information and spectral efficiency of the modulation scheme. The spectral efficiency is measured in bits per hertz. The baseband is multiplied by a carrier frequency, resulting in a frequency shift in the amount of the carrier frequency. This signal is amplified with an RF amplifier and is transmitted via an antenna. Before the signal is received by the receiving station, the electromagnetic waves carrying the information are distorted by the wireless channel.

The wireless channel is characterized by various time-variant and time-invariant parameters. This section gives only a short introduction to the characteristics of the wireless channel. The properties of the mobile wireless channel can be roughly characterized by the following two attributes:

- **Large-scale fading**: This is due to loss of signal strength by distance and shadowing of large objects like hills or buildings. It is typically frequency independent, but a function of time and space which fluctuates by means of cell areas.

- **Small-scale fading**: This is due to the constructive and destructive interference of the multiple signal paths between the transmitting node and the receiving one, resulting in signal strength changes on a spatial scale of the wavelength. Therefore, signal strength variation greatly increases with faster moving stations and is frequency selective.

Free space attenuation as a function of distance d and wavelength λ is shown in the following equation. This basic attenuation (part of large-scale fading) denotes the signal decrease between source and destination without taking any shadowing, multipath fading, or scattering into account:

$$L = 10 \log \left(\frac{4\pi d}{\lambda} \right)^2 \text{[dB]}$$

Especially, the small-scale fading introduces distortion in the received signal to such an extent that it needs to be eliminated, or at least reduced by entities called channel estimator and channel equalizer described later in this section.

Figure 1.29 shows a typical received wireless channel quality as a function of frequency and time. The channel quality (received signal strength of certain frequencies) changes on a large scale (large-scale fading) and is superposed by the small-scale fading of a moving node. The physical layer of mobile wireless transmission systems have to deal with these characteristics of mobile channels to ensure data transmission to a specific subscriber velocity. Because small-scale fading spatially changes by means of the wavelength, typically by several centimeters in mobile networks, the user velocity introduces fast fading to the received signal. As an example, a user velocity of 100 km/h

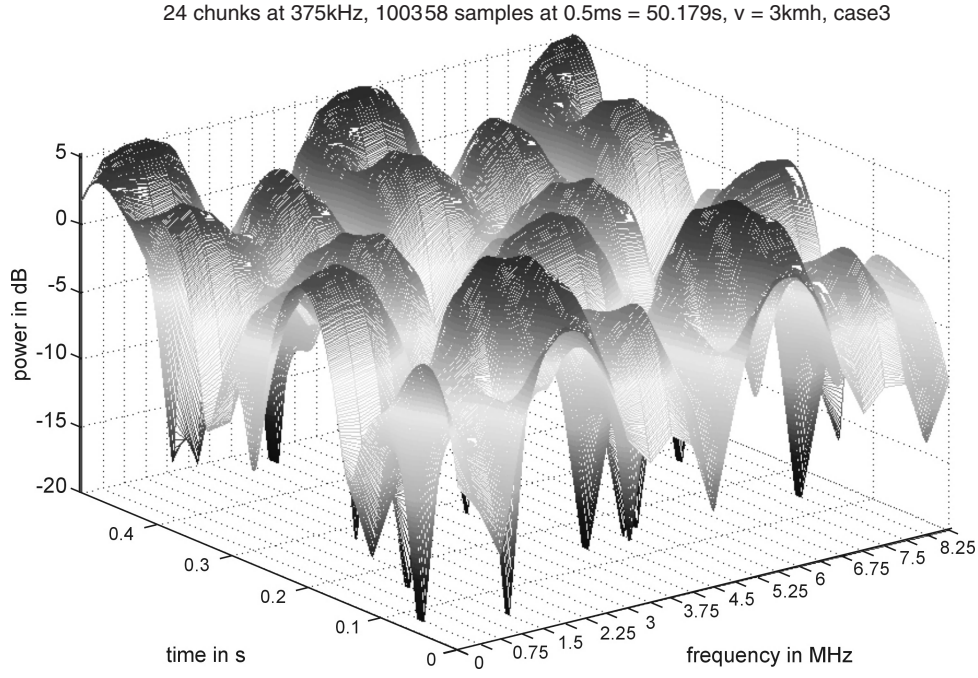


Figure 1.29 Time-variant frequency-selective wireless channel. Reproduced with permission from Nomor.

(27.8 m/s) can result in signal fading changes of 250 times a second. As a result, the received signal is additionally amplitude modulated (a fast amplitude change) caused by the fast fading of a moving user. The amplitude modulated due to the time-variant wireless channel causes additionally frequency dispersion. Entities like fast power control and fast frequency-selective scheduling (see Sections 1.8.7 and 1.8.9) are introduced into mobile systems in order to counteract this.

A multipath channel is time dispersive, which means that a single transmitted signal is received more than once with different strong echoes (reflections). The electromagnetic waves are reflected by obstacles like buildings, hills, and mountains. The direct beam between the transmit antenna and receiver is called the LOS (Line Of Sight). The LOS is usually the strongest pattern within the brought field of received reflections. $h(\tau, t)$ is the time-variant (t and τ) impulse response of the wireless channel with i paths (reflections) and an attenuation $a_i(t)$ of each path i. The impulse response denotes the characteristic behavior of a system (in a mathematical sense), like the wireless channel when an impulse (delta peak) is given as input. In theory, this impulse is so steep that all possible frequencies are included, thus it shows the behavior of all transmitted patterns. τ is the delay of the signal between the source and receiver. This delay is called the propagation delay. τ_i is the additional delay of the reflection path i. Thus,

$$h(\tau, t) = \sum_{\forall i} a_i(t)\delta(\tau - \tau_i(t))$$

The transmitted baseband signal is distorted by the wireless channel because different reflections of the signal are interfering at the receiver. Thus, the time-continuous received complex baseband signal $y_b(t)$ of a transmitted signal $x_b(t)$ with additive white Gaussian noise $n(t)$ is

$$y_b(t) = \sum_{\forall i} a_i(t) \exp[-j2\pi f_c \tau_i(t)] x_b(t - \tau_i(t)) + n(t)$$

f_c is the frequency which is used to transmit the information. It is referred to as the carrier frequency, as mentioned above. The term $\exp[-j2\pi f_c \tau_i(t)]$ denotes the time-variant phase shift of each reflection path i.

By knowing the distortion $h(\tau, t)$ which was applied to the received signal due to wireless transmission, the receiving entity is able to reverse this distortion and retrieve the transmitted information. In order to estimate the wireless impulse response by the receiver, the transmitter entity inserts known patterns into the transmit signal. Those signals are referred to as pilot or reference signals. Additionally, pilot, reference, or synchronization signals can be applied for time and frame synchronization (in LTE special synchronization signals are used, see Section 1.8.15). The receiver scans the received signal for the pilot or synchronization signals by using correlation functions. Once frame synchronization is established, the channel estimator unit of the receiver analyzes the known signal part in order to estimate $h(\tau, t)$.

The channel estimator passes the results of the process of estimation to the channel equalizer. The channel equalizer is the entity which removes the distortion due to wireless transmission. Thus, the quality of channel equalization depends on the provided information of the estimator unit. Almost every mobile cell phone standard uses different estimators and equalizers depending on the structure of reference symbols and slot structure. In LTE, channel estimation and equalization are done in the frequency domain and interpolated between adjacent time domain transmission symbols, resulting in a two-dimensional channel equalization. The process of channel estimation and equalization used in LTE is described in Sections 1.8.6 and 1.8.15.

1.8.1 Duplex Methods

A valuable communication feature is bidirectional communication between peers. Feedback is the major difference to unicast or broadcast systems, such as TV or radio transmission. Bidirectional

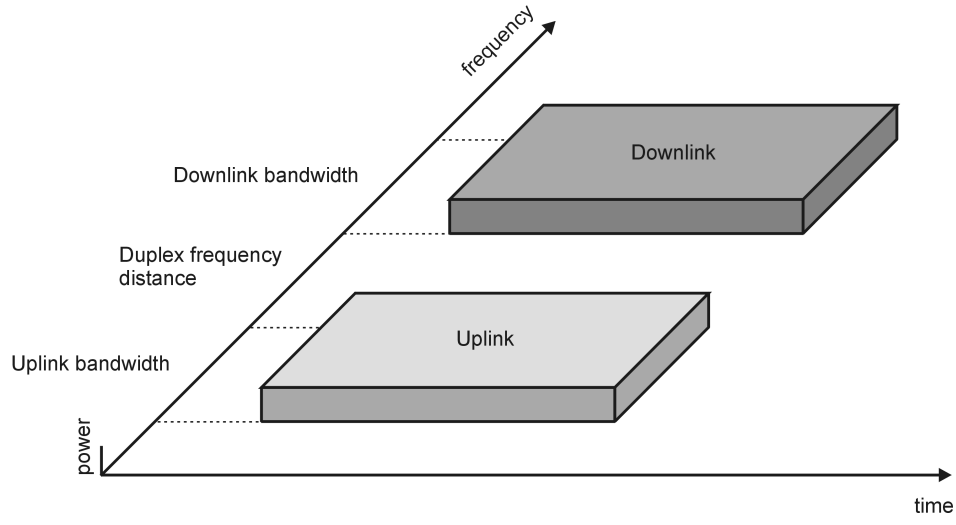


Figure 1.30 FDD system.

information transfer can occur either simultaneously or consecutively. Both in data networks and especially for human communication, simultaneous bidirectional communication is very basic and essential. Systems with the nature of simultaneous bidirectional information transfer are full-duplex systems, in contrast to half-duplex systems, which allow only one-by-one bidirectional communication.

A full-duplex application visible to the user does not need to imply a full-duplex transmission scheme on lower layers. In mobile networks two basic methods of multiplexing and handling the duplex streams are used. Here duplex means the sense of UL and DL transmission from the handset to the base station and vice versa.

Frequency Division Duplex (FDD) divides the available frequency spectrum in a frequency range dedicated to UL transmission and a separate range for DL transmission only. A guard band is used between the frequency bands allocated for the UL and DL direction in order to prevent UL and DL interference. Figure 1.30 depicts a divided frequency spectrum as is typically used with FDD.

Time Division Duplex (TDD) makes use of the same frequency resources for both transmission directions. This method divides the time domain into slots allocated for UL and DL transmission as shown in Figure 1.31. A guard interval is implemented to prevent UL and DL interference, especially for larger cells with a longer propagation delay spread (larger cells have a longer duration behavior until all echo reflections of the transmitted signal are received) and cases of non-ideal UL synchronization.

TDD defines various slot configurations of switching between UL and DL transmission (see Table 1.10). Different configurations are possible depending on the mixture between UL and DL traffic; usually the UL data volume is much smaller compared to DL data consumption. A change in transmission resources for the UL and DL direction are just one manner of soft system configuration with TDD, instead of FDD, which uses fixed frequency resources.

TDD systems have the advantage of a synchronous channel between the UL and DL direction because the wireless channel characteristic is frequency dependent and TDD uses the same frequency band for UL and DL transmission. This is especially interesting in systems which use frequency-selective scheduling (see Section 1.8.7) and smart antennas (MIMO (Multiple Input, Multiple Output) transmission with multiple antennas) as they are defined in LTE. The base station needs to know the reception conditions of the UE in order to make an efficient frequency resource scheduling decision and for selecting the best antenna configuration for multiple antenna layer precoding.

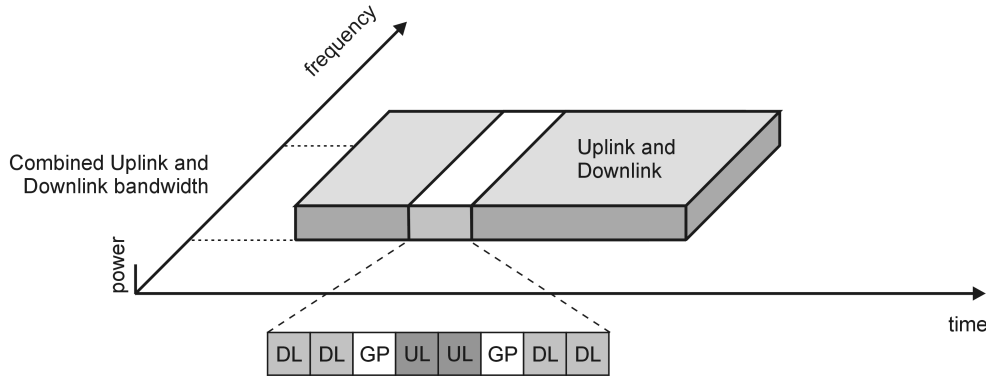


Figure 1.31 TDD system with example duplex slot structure.

1.8.2 Multiple Access Methods

Multiple access has to be performed in systems where a medium is shared for transmission and reception by multiple users or entities. Those entities or users, sometimes also called nodes, are accessing the very same medium to transmit their information, other than, for example, in CS communication schemes. For example, within classical CS communications like Plain Old Telephone Systems (POTSs), each communication node gets a dedicated resource (a telephone landline) to dedicatedly access for the complete communication session. On the other hand, it is necessary to apply a multiple access method when multiple nodes share the same medium for their information transfer, in order to prevent or detect collisions on the shared medium.

This implies that the users share the same resources for communication in a certain way. Multiple access methods are mainly used with PS data transmission, as multiple nodes usually share the same resources for efficiency reasons. Packet Switched (PS) data transmission is mostly characterized by bursty traffic patterns. There are different schemes which can be applied to share those resources. These access schemes are known as multiple access methods.

Multiple access methods introduce rules for accessing the shared medium, generally resources. Care has to be taken not to use the same resources by two or more nodes at once, because this would result in distortion of the transferred information.

Transmission/reception resources are one or multiples of the following: time, code, frequency, space, etc.

One of the first radio-based multiple access scheme is Aloha. Early research in these schemes was carried out at the University of Hawaii in the early 1970s. In the Hawaiian language *Aloha* means “Hello” which indicates a fundamental mechanism: the university ran several campuses on different islands where an early radio-based packet data network was established. Stations immediately transmitted packets to be sent and waited for a fixed time (double the round-trip time of the most distant stations in the network plus the transmission and processing time of packets) for an acknowledgment (ACK) from the receiving station. If an ACK was received, the packet was retransmitted. Aloha shows that many collisions of packets occur when applying this scheme.

Most modern access methods use mechanisms of avoiding, detecting, or preventing collisions within the shared medium, in order to reach a certain system efficiency. A basic method to avoid collisions is sensing the medium before starting a transmission, to avoid interrupting or interfering with an ongoing transmission of other communication peers.

This scheme is known as Carrier Sense Multiple Access (CSMA). Sensing the medium before transmission adds Collision Avoidance functionality (i.e., CSMA/CA). In addition to sensing the

medium before transmission, one has to take care with detecting collisions when two terminals have started a transmission at the same time. This scheme, for example, is used with Ethernet local area networks, CSMA/CD. If a collision is detected from both transmit entities, a collision resolution mechanism must be applied. Both peers select a random time in a defined range in order to restart their transmission after this randomly selected period of time. The process starts by sensing the medium again, as the other collision peer (or a new transmission of a third node) could already have (re)started its transmission as it has selected a shorter back-off period. The efficiency can be increased by introducing discrete back-off slots.

A special effect of wireless networks without infrastructure has to be taken care of. As mentioned above, a station listens to the channel before sending data to avoid a collision with an ongoing transmission from two other stations at that time. But this behavior is not fully sufficient to avoid collisions at all stations within the transmission range. If a node within the transmission range receives a data frame from another station which is not in the range of a node also trying to allocate the channel, this node will interfere with reception of the other node without warning. This unrecognized collision scenario is called the hidden terminal effect, because the sending node is "hidden" or out of range.

Figure 1.32 shows a typical scenario for the hidden terminal effect. The circles around the stations demonstrate the transmission ranges of the nodes. Node A has a link to node B but does not know about the existence of node C, which is the hidden terminal from the point of view of node A. Node B has a link to both node A and node C. In this scenario node C attempts to transmit data to node B and indicates this with a Request to Send (RTS) packet with the destination address of node B. The designated destination node B confirms this request with a Clear to Send (CTS) packet to node C; this CTS packet is also received by node A. Thereby, node A detects that there is another station while transmitting, until the reception node B sends an ACK packet to complete this transmission. Within

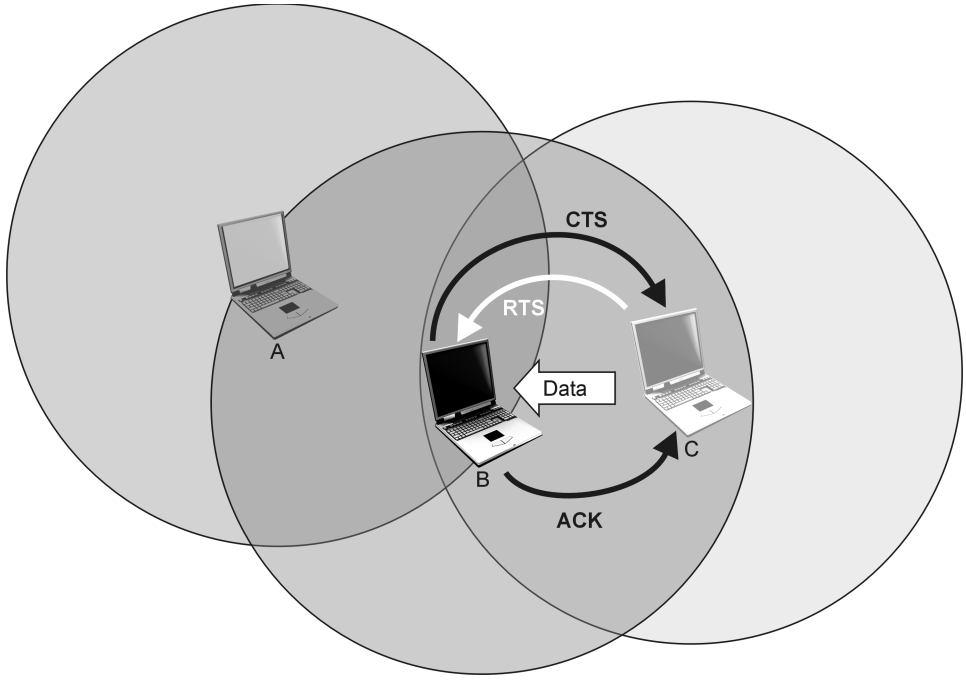


Figure 1.32 Illustration of the hidden terminal effect.

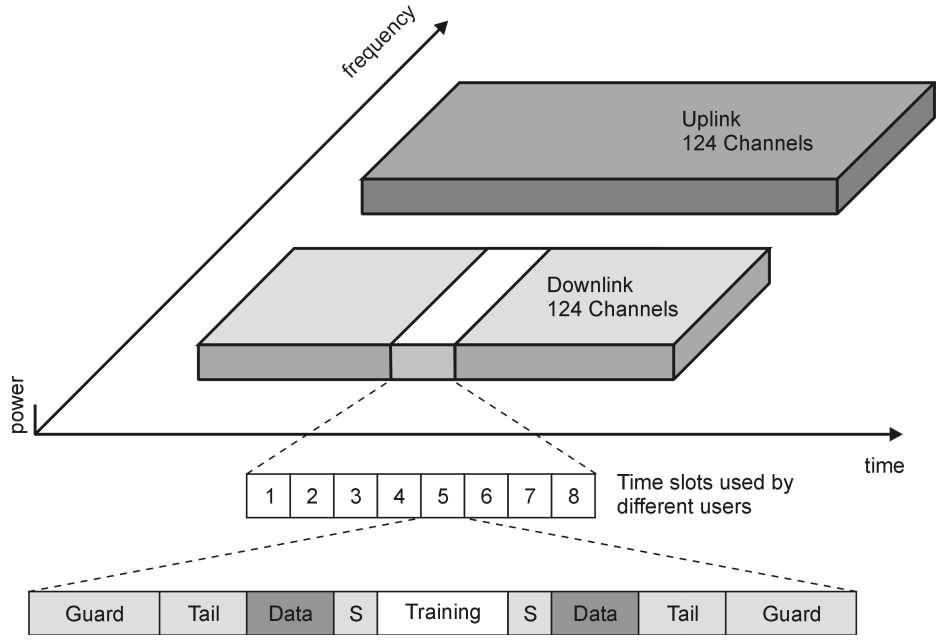


Figure 1.33 Schematic example of a Time Division Multiple Access (TDMA) system.

that time, node A will not initiate any transmission, not to node B nor to any other possible node, in order not to corrupt reception at node B.

Note that this effect only occurs in mobile networks without fixed infrastructure, for example, mobile ad-hoc networks. Thus, the hidden terminal effect does not affect LTE.

One way of sharing the same resources between communication entities is to introduce a master entity, which takes care of the usage of the shared medium. This scheme is widely used within mobile cell phone networks, as the base station controls and grants the access of resources within its cell. Within a Time Division Multiple Access (TDMA) mobile network, one frequency resource is divided into time slots which are used by different users. Mobile networks of the second generation (GSM) share eight time slots within a certain frequency band. Figure 1.33 illustrates the DL frame of a TDMA system which uses FDD. Thus, UL and DL utilize different frequency bands and both use TDMA. A Guard Period (GP) used between time slots serves to reduce the risk of multi-user interference. The training sequence in the middle of the time slot is used to estimate the wireless channel conditions. This information is extrapolated time-wise to the adjacent data sections.

Non-overlapping frequency bands are assigned to different UEs within Frequency Division Multiple Access (FDMA). A single user allocates one frequency resource which is used for the complete active time. Guard bands need to be designed for the system in order to prevent multi-user interference. Systems (as GSM) often use a mixture of TDMA and FDMA, as multiple frequency channels with, for example, eight time slots serve as cell resources. Figure 1.34 depicts a FDMA system with five users assigned to five different frequency bands.

UMTS users share orthogonal codes which are used to spread transmission data in order to be transmitted on the same frequency resources within one cell. Picture this as a metaphor: each user uses the same time, space, and frequency resources, but communicates in a different language. This multiple access method is known as Code Division Multiple Access (CDMA) and illustrated in Figure 1.35.

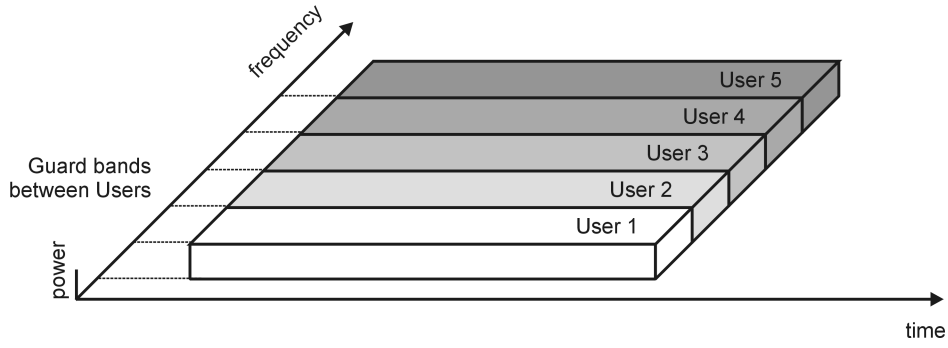


Figure 1.34 Schematic of Frequency Division Multiple Access (FDMA).

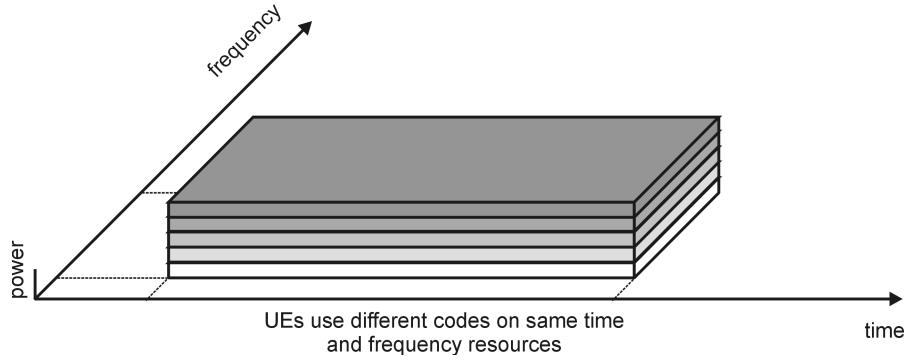


Figure 1.35 Code Division Multiple Access (CDMA).

The shared resources in LTE are very small frequency bands and small transmission time slots. Thus, the method combines FDMA and TDMA behavior, but in a very agile way. Frequency and time resources are often reassigned for diversity or efficiency reasons during ongoing user transmissions. This method is known as Orthogonal Frequency Division Multiple Access (OFDMA). OFDMA is described in Section 1.8.4 in detail, as well as OFDM signal generation and characteristics in Section 1.8.3.

Within mobile cell phone network systems, time slot resources, frequency resources, and code resources are controlled by the base station. This controlled multiple access method is known as scheduling. The scheduling method applied in LTE is described for the DL direction in Section 1.8.7 and for the UL in Section 1.8.9. This scheduling case allows active transmission collision protection, as well as other parameters, to be taken into account when granting transmissions between users. These parameters can be fairness, QoS requests of nodes, medium/channel quality or (charging) policies. Details on scheduling parameters are found in the above-mentioned sections.

1.8.3 OFDM Principles and Modulation

Most recent communication systems like WiFi, WiMAX, and digital audio and video broadcasts make use of OFDM, as in the LTE DL transmission scheme and a slightly modified version in the LTE UL transmission scheme.

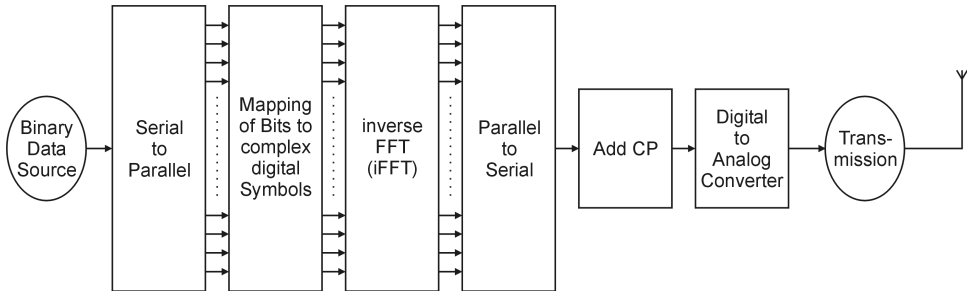


Figure 1.36 Block diagram of OFDM signal generation.

OFDM systems have some advantages for mobile wireless transmission as signals are robust against frequency-selective fading. Systems which make use of OFDM have been known since the 1950s and 1960s in military applications. Their realization was expensive as all components and filters were implemented as analog circuits. Nowadays, a wide range of applications profit from the benefits of OFDM systems since digital signal processing has become inexpensive and available in consumer products.

Information is modulated on very small adjacent carriers within the allocated bandwidth (baseband). The intrinsic design of an OFDM system prevents interference among the carriers (also called subcarriers or tones). This is the reason why the subcarriers are orthogonal to each other. Figure 1.36 shows the basic components needed for OFDM signal generation. The realization of an OFDM signal generator and analyzer is simple to achieve as the main computational functions are transformations between time and frequency spectra which are easy to implement in modern digital signal processing integrated circuits by using the Fast Fourier Transform (FFT) algorithm.

The first step in the transmit chain is the serial-to-parallel conversion of the data to be transmitted. This is usually done within the transmit buffer. This binary data is now quadrature amplitude modulated by mapping bits to complex data symbols. The characteristic of complex data symbols is that each symbol describes a two-dimensional vector with a phase and amplitude. A complex data symbol is described with an in-phase and a quadrature component. These symbols are called IQ samples, as the modulated symbols are digitally sampled. Figure 1.54 in Section 1.8.11 depicts the modulated complex QAM symbols (modulation schemes) and the corresponding bit mappings. It is possible to map a higher number of bits to symbols by using a higher modulation order like 16 or 64QAM resulting in a higher spectral efficiency, which means transmitting more bits per hertz of the utilized bandwidth. A higher spectral efficiency allows greater user and cell data throughput. The number of bits which are carried by the different modulation schemes can be seen in Table 1.7. Those numbers are OFDM independent and are equal to other transmission schemes.

Table 1.7 Bits to be carried by the modulation schemes used with LTE

Modulation scheme	Number of bits which can be carried by one complex symbol
BPSK	1
QPSK	2
16QAM	4
64QAM	6

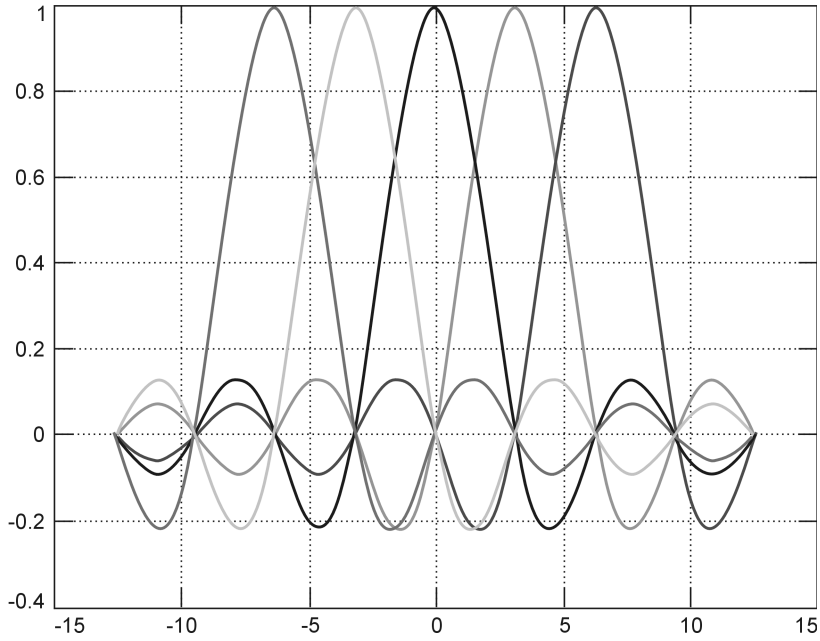


Figure 1.37 OFDM signal of orthogonal Si functions (subcarriers); subcarriers do not interfere because at each subcarrier the signals from other subcarriers are zero.

Mobile cell phone standards which do not use OFDM, like GSM, CDMA2000, or UMTS, modulate the data to complex symbols in the time domain. This means that the resulting sinusoid over time after modulation is the time domain signal of the baseband to be transmitted on the RF carrier frequency. OFDM systems interpret the modulated symbols as modulated frequency tones, which are to be transformed to a signal over time in order to be transmitted. Thus, the modulated symbols are mapped to orthogonal subcarriers (tones) of the baseband spectrum. The transformation to the time domain is done with an n-point inverse Fast Fourier Transform (iFFT). The Fourier transformation adds the orthogonal spectrum of each subcarrier to the resulting baseband spectrum. The spectrum of each subtone is a $si(x)$ function $(\sin(x)/x)$, thus the resulting spectrum is an addition of $si(x)$ functions as depicted in Figure 1.37. The inherent behavior of the Fourier transformation lets each $si(x)$ maximum match zero transitions of all other $si(x)$ functions, resulting in non-interfering subtones since the data was modulated to individual subcarriers (peaks of the $si(x)$ functions). This characteristic is known as orthogonal behavior, which means data is perfectly demodulatable and no guard band between subcarriers is needed, in contrast to FDM, where intercarrier interference needs to be taken care of, for example, with guard bands.

The designated system bandwidth (baseband bandwidth) is divided into m subcarriers which are sampled with an n-point Fourier transformation, where $n > m$, indicating oversampling. System bandwidth is defined by a number of resource blocks (see Section 1.8.5) from 6 to 110, each resource block grouping 12 subcarriers. For approximately 20 MHz system bandwidth (100 resource blocks), 1200 subcarriers are defined and a common FFT size is 2048 samples. LTE defines the sampling frequency as $f_s = 1/T_s = 30.72\,\text{MHz}$, which leads to a LTE OFDM symbol length of 66.67 µs for normal CP (Cyclic Prefix). The CP is 5.2 µs or 160 samples in the first symbol and 4.7 µs or 144 samples in the other symbols for normal CP. The CP lasts 16.7 µs or 512 samples for extended CP. Details of LTE slot definitions are given in Section 1.8.6.

Ex.1013.00058

OFDM systems show robust characteristics against frequency-selective fading caused by the wireless channel, because fading holes are bigger compared to the subcarrier bandwidth, leading to a flat fading of individual subcarriers which is equalized by interpolating between defined reference symbols (reference subcarriers).

LTE defines a set of reference symbols in order to distinguish between various entities: cell-specific, UE-specific, antenna-port-specific, and MBMS-specific (Multimedia Broadcast/Multicast Service) reference symbols. MBMS data and reference symbols are always transmitted on antenna port 4 if MBMS data transmission is enabled.

In other words, the time domain is just the "transmit domain" for OFDM systems. The resulting time domain signal after transforming the modulated frequency signal representing the data is, so to say, "just noise" and cannot be interpreted without transformation back to the frequency domain. All channel estimation, equalization, and interpretation of the data are done in the frequency domain within OFDM systems.

A timely guard interval or GP between OFDM symbols is needed to prevent intersymbol interference due to channel delay spread (arrival of all reflections). This is realized by copying the end of each OFDM symbol in front of the OFDM samples to be transmitted. This GP, also known as the CP (Cyclic Prefix), decreases alias effects caused by a windowing effect of the Fourier spectrum as the Fourier transformation expects an infinite repeated spectrum, but the OFDM symbol has a time-limited duration. LTE defines two CP lengths, a normal CP and an extended CP, for cells with a larger channel delay spread. Additionally, the CP is used for frame synchronization using an auto/cross-correlation function.

OFDM systems have the drawback of a high dynamic range after transforming the frequency signal to a time domain signal which is amplified and transmitted. This high Peak-to-Average Power Ratio (PAPR) (squared peak signal amplitude to average signal power level) leads to cost-intense RF amplifiers and shorter battery life. This is especially a disadvantage for mobile handset devices; thus, another transmission scheme needs to be found for the UL.

LTE uses Single Carrier Frequency Division Multiple Access (SC-FDMA) or Discrete Fourier Transform (DFT) spread OFDM as the UL transmission scheme to overcome some drawbacks of pure OFDM systems. SC-FDMA is described in more detail in Section 1.8.8.

Figure 1.38 presents an overview of the functional steps needed for physical channel processing.

1.8.4 Multiple Access in OFDM – OFDMA

LTE uses OFDM as the transmission scheme, as described in the section above. Multiple access, as introduced in Section 1.8.4, is realized with OFDMA with the base station (eNB) taking care of the resources within its cell; this procedure is also called scheduling as the eNB schedules the transmission

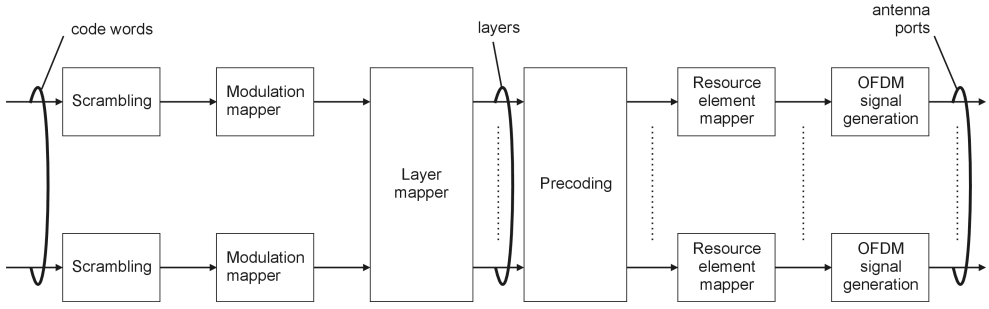


Figure 1.38 Overview of physical channel processing. Reproduced with permission from © 3GPP™.

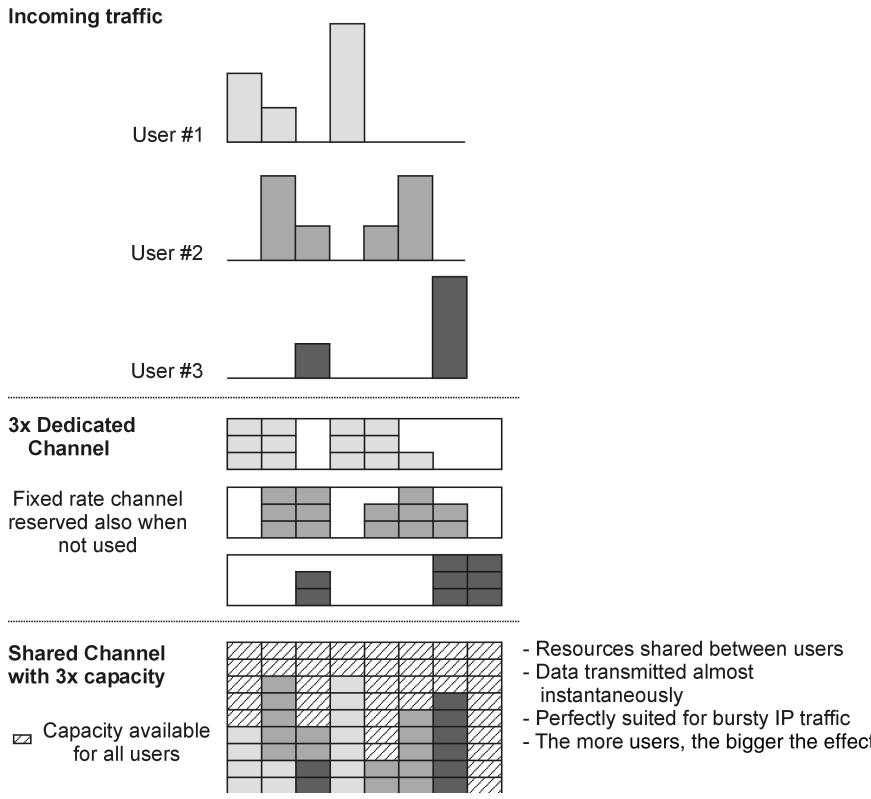


Figure 1.39 OFDM shared channel-based multiple user communication. Reproduced with permission from Nomor.

of user data in the DL and UL direction on the transmission medium used by all users within this cell. The transmission is done on the basis of a shared channel. The control information for granting an UL transmission on the UL-SCH, or informing a UE about data that is transmitted for it on the DL-SCH, is done within the DL control channel with designated control information. Physical channels defined with LTE are described in more detail in Section 1.8.12. Figure 1.39 shows the principle of an OFDM shared channel-based multiple user communication.

Resources to be scheduled with OFDMA systems are units of frequency resources and time units describing a time slot for which the scheduled frequency units are valid.

This scheduling procedure not only adds overhead, but also enables the system to be more efficient by introducing a frequency-selective scheduling algorithm with feedback from the UEs regarding current reception quality, rather than use only diversity gains by spreading transmitted data.

Figure 1.40 compares a shared channel of an OFDMA system using localized and distributed scheduling of user data. In the localized mode, granted areas belonging to one user allocate adjacent frequency resources within one block. The distributed mode is used when frequency diversity is to be used by spreading the user data of the shared channel to distributed non-adjacent frequency resources. Simulations show that systems with frequency-selective scheduling with a fast channel quality feedback report from users can achieve higher cell throughput compared to systems just spreading data over the spectrum in order to achieve frequency diversity.

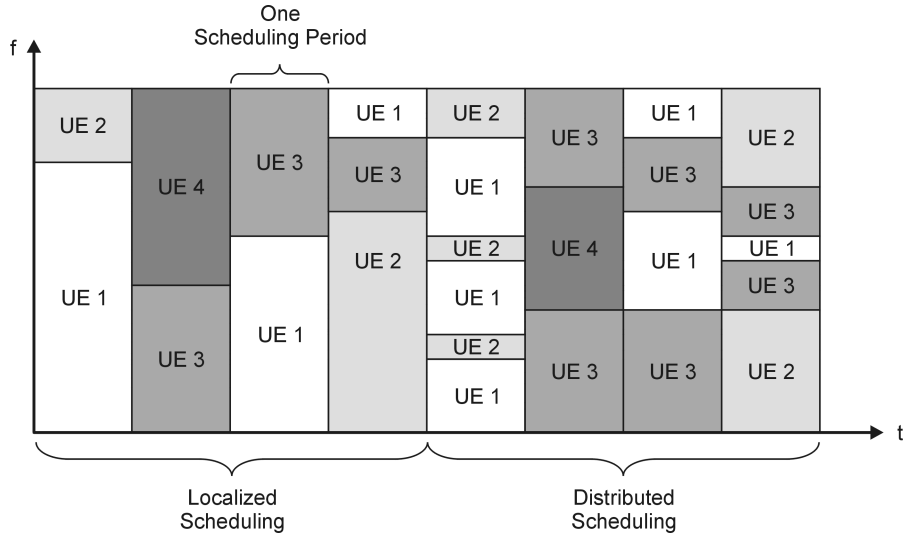


Figure 1.40 Localized vs. distributed shared channel scheduling.

LTE defines both localized and distributed scheduling in the DL direction but only localized scheduling in the UL direction in order to keep the PAPR small in the SC-FDMA symbols of each user. Details of scheduling the LTE DL can be found in Sections 1.8.7 and 1.8.9, which describe the LTE UL scheduling.

1.8.5 Resource Blocks

This section describes how LTE defines and divides the bandwidth from physical subcarriers of the OFDM symbol in the logical abstract sense used for scheduling shared channel data.

The smallest division of the LTE spectrum carrying data is a subcarrier, as described in more detail in the sections above. OFDM systems modulate all data in the frequency domain on the subcarrier of the OFDM spectrum. A modulated subcarrier is defined as a Resource Element (RE) and is the smallest logical unit of the LTE spectrum. One subcarrier or RE has a bandwidth of 15 kHz in normal and extended CP mode, but a special 7.5 kHz subcarrier spacing mode is defined with extended CP transmission. All physical LTE channels use REs to modulate the data. Each RE of the shared channel is modulated using a variable modulation scheme from Quadrature Phase Shift Keying (QPSK) to 64QAM as assigned by the scheduling process of the eNB. REs carry a variable number of data bits, due to the variable number of bits mapped to a RE because of the modulation order, but also because of applied CSs. CSs are used to make the data transmission more robust against transmission errors. They add redundancy to the transmitted information, which increases the probability of the receiver to retrieve the information error-free. LTE defines an Adaptive Modulation and Coding (AMC) process, which is described in Section 1.8.11 in more detail.

A physical Resource Block (RB) defines the smallest unit used by the scheduling algorithm. Therefore, the minimal scheduled user transmission on the shared channels is one RB. A RB consists of 12 adjacent REs on the frequency axis. Consequently, it has a bandwidth of 180 kHz, since one RE is 15 kHz wide in normal and extended CP mode (additionally a mode with 7.5 kHz is defined for extended CP). The possible configurations of CPs are given in Table 1.8.

Table 1.8 Configuration of cyclic prefix. Reproduced with permission from © 3GPP™

Configuration		N_{sc}^{RB}	N_{symb}^{DL}
Normal cyclic prefix	$\Delta f = 15\,\text{kHz}$	12	7
Extended cyclic prefix	$\Delta f = 15\,\text{kHz}$	24	6
	$\Delta f = 7.5\,\text{kHz}$		3

From a time perspective, a RB spans one scheduling period which is defined as one subframe. One subframe has a duration of 1 ms. A subframe is divided into two slots of 0.5 ms. Within a subframe 14 OFDM symbols are transmitted in the case of normal CP length and 12 OFDM symbols in the case of extended CP length, hence a RB covers an area of, respectively, 12×14 and 12×12 REs. The time-wise LTE slot and frame structure is described in Section 1.8.6.

A third dimension is introduced by using multiple antenna ports with MIMO. The MIMO transport layers depend on and correlate with the number of used transmit antenna ports. Each antenna port layer adds additional RB elements to the antenna port dimension. Figure 1.41 shows the two-dimensional (frequency and time) area of a RB.

RBs have a primary role in the scheduling process, but are also used for describing the LTE overall cell bandwidth. The cell bandwidth is announced in the data transmitted in the Physical Broadcast Channel (PBCH) in number of resource blocks. Table 1.9 maps the number of RBs to the LTE spectrum bandwidth in megahertz.

The scheduling procedure defines virtual resource blocks. Virtual resource blocks and physical resource blocks are of equal size. The scheduler always uses virtual resource blocks for defining user allocations. There are two different types of virtual resource blocks:

- Localized virtual resource blocks.
- Distributed virtual resource blocks.

Localized virtual RBs are equal to physical RBs. Therefore, localized virtual RBs address physical RBs directly. Distributed RB mapping enables the usage of frequency diversity without scheduling distributed RBs directly. Distributed virtual RBs split a physical RB at the slot boundary into two halves. The first half of the scheduled distributed virtual RB directly equals the physical RBs. The second slot is hopped to another second slot of another UE which is virtually scheduled in the distributed way. There is one hopping gap between the scheduled RBs at system bandwidths smaller 50 RBs and two gaps at systems with a larger number of RBs. Virtual RBs are used with resource allocation type 2 described in Section 1.8.7.

Resource Element Groups (REGs) are defined to map physical channels to OFDM symbols, this is done especially in the first OFDM symbols used by the PDCCH. The maximum length of the PDCCH is three OFDM symbols, thus other PHY channels are mapped into the resources of the PDCCH. A REG is defined in such a way that it spreads the information over a bigger frequency range to gain frequency diversity. Figure 1.59 in Section 1.8.12 illustrates REGs in the PDCCH.

1.8.6 Downlink Slot Structure

This section introduces the LTE DL structure with respect to time. In the time domain, the DL is divided into slots and frames. A radio frame is the largest unit and lasts 10 ms. As both duplex modes, FDD and TDD, use similar timings, this makes a UE starting to synchronize to a LTE cell unaware of the duplex method used. Thus, TDD and FDD both introduce radio frames of 10 ms timing.

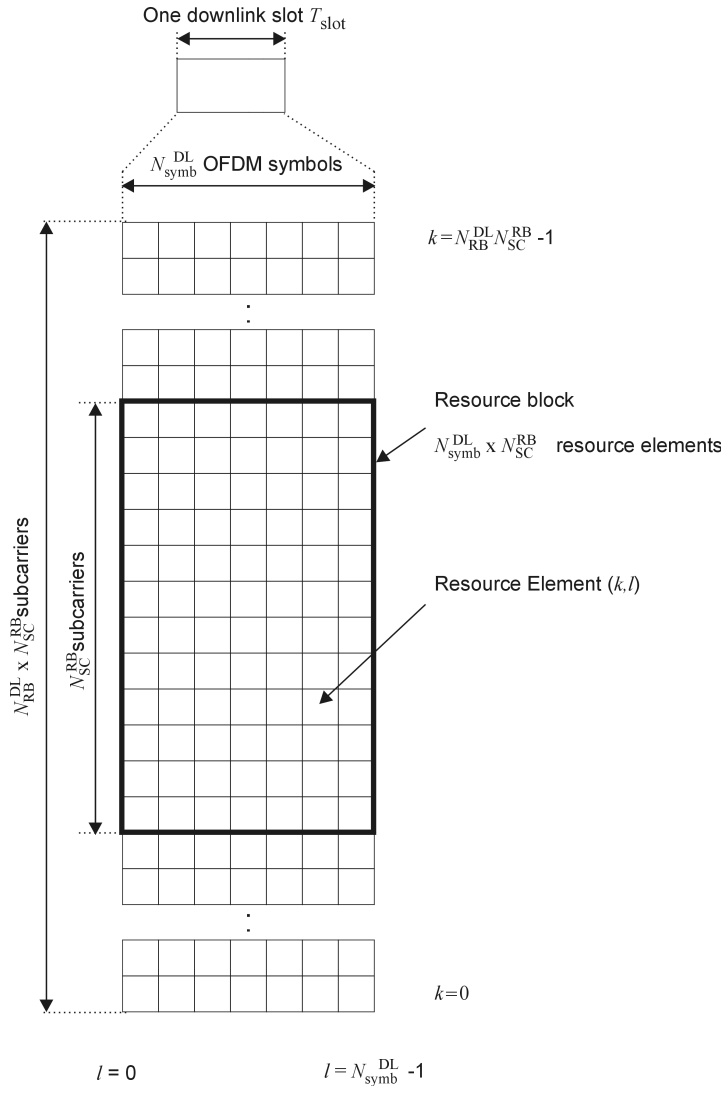


Figure 1.41 Downlink resource grid. Reproduced with permission from © 3GPP™.

Table 1.9 Commonly used number of resource blocks

Bandwidth (MHz)	Resource blocks
1.4	6
3	13
5	25
10	50
15	75
20	100

Both duplex methods define different types of radio frames:

- Frame type 1 is the frame type used with FDD.
- Frame type 2 is the frame type used with TDD.

One radio frame is split into 10 subframes of 1 ms duration. A subframe is also the most important unit of scheduling and for physical control channel durations the PDCCH is found in the first OFDM symbols of each subframe. Furthermore, subframes are divided into two slots of 0.5 ms. The smallest unit is an OFDM symbol. Depending on the CP length (normal or extended) used (see Section 1.8.3), the length will be seven or six OFDM symbols transmitted within one slot, resulting in 14 or 12 OFDM symbols within one subframe, respectively. Figure 1.42 shows one radio frame of type 1 (FDD) with 20 slots and 10 subframes. The length of one radio frame is defined as $T_f = 307\,200 \times T_s$ where T_s is the sampling period. Therefore, the base sampling frequency of 30.72 MHz ($T_s = 1/30.72\,\text{MHz}$) is used.

Figure 1.43 shows a complete radio frame of type 1 as used with FDD. It illustrates all 10 subframes with areas for the PDSCH. The first OFDM symbols are allocated by the PDCCH. In the area of the PDCCH, additional physical channels for control information are embedded. These channels are the Physical HARQ Indicator Channel (PHICH) and the Physical Control Format Indicator Channel (PCFICH).

The PCFICH indicates the number of OFDM symbols allocated for the complete PDCCH in its current subframe. Thus, the PDCCH is transmitted on a variable number of OFDM symbols depending on how much control or scheduling information has to be transmitted, and the resulting number of OFDM symbols which are used for the PDSCH is variable as well. The PDCCH allocates between 1 and 3 OFDM symbols and the PDSCH between 13 and 11 for normal CP and between 11 and 9 OFDM symbols for extended CP, respectively.

In the middle (around the DC subcarrier) of the bandwidth are six RBs used for some common signals and channels in some subframes. These locations are used for initial cell search and cell synchronization. This central location enables a bandwidth-independent cell and frame synchronization as well as initial cell access. Two step hierarchical synchronization signals are defined and located in the first and sixth subframes. The Primary Synchronization Signal (PSS) is transmitted on the seventh OFDM symbol and the Secondary Synchronization Signal (SSS) is transmitted on the sixth OFDM symbol of subframes described above. PSS and SSS can be seen in Figure 1.43 and Figure 1.62 shows the bandwidth of the synchronization signals. Only 62 subcarriers of the 72 provided by six allocated RBs are used for synchronization signals. Initial UE radio access is described in Section 1.8.15 as well as the information carried by those signals.

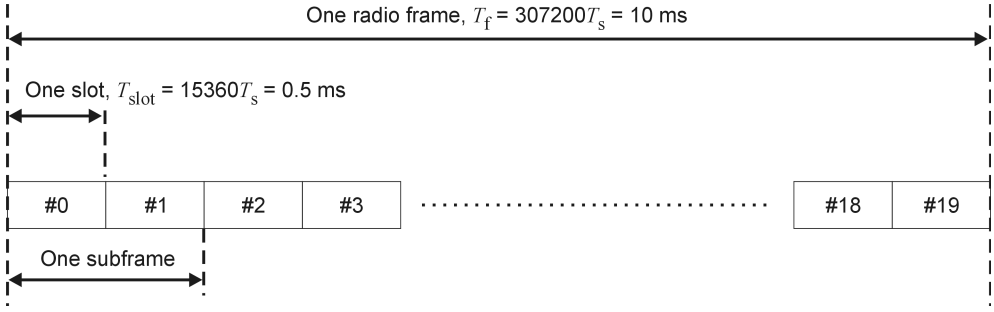


Figure 1.42 Frame structure type 1 used with FDD TS36.211. Reproduced with permission from © 3GPP™.

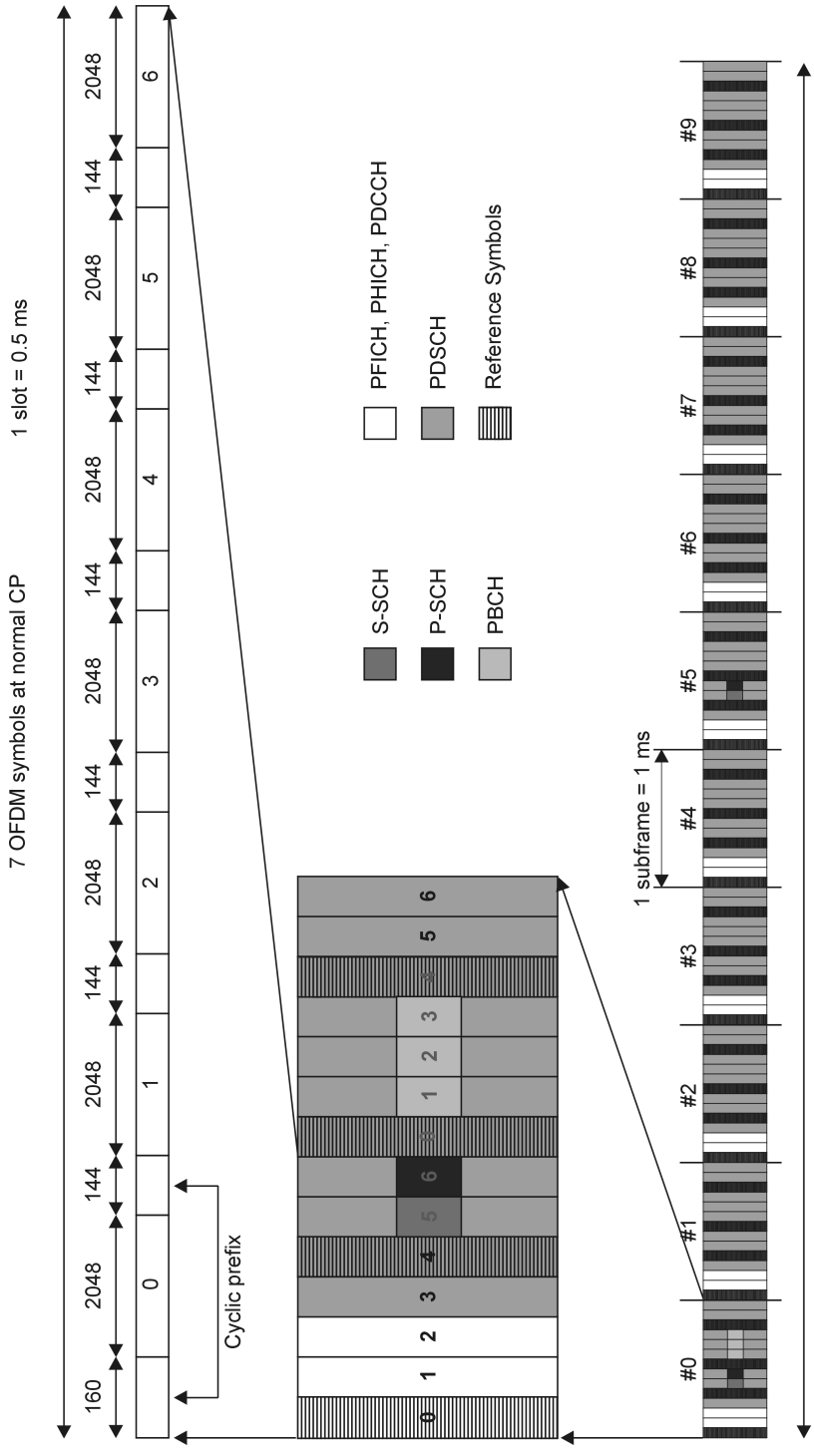


Figure 1.43 Downlink FDD radio frame (normal cyclic prefix) with PDCCH, PDSCH, PBCH, reference signals, and synchronization signals. Reproduced with permission from Nomor.

Resources for the PBCH are allocated apart from the SSS. The PBCH is transmitted in each first subframe of all radio frames. Other than the synchronization signals, the PBCH uses all 72 subcarriers of the six central RBs (see Figures 1.43 and 1.62).

Reference signals are needed by the channel estimation process in order to correct the wireless channel distortion in the signal at the receiver. Four sets of reference signals are specified for each transmit antenna as LTE defines multi-antenna transmissions (DL MIMO). The receiver needs to know the propagation conditions of each transmit antenna for using the complete MIMO gain. Therefore, a defined signal (reference signal) is transmitted from each individual antenna completely independently and all other transmit antennas do not transmit any signals on those specific frequencies and time resources (REs). Figure 1.44 illustrates the frequency and time RE used for transmitting reference signals depending on the number of antennas configured.

Frame type 2 is used with TDD. The general slot structure of a TDD frame is similar to a FDD frame, since a mobile is not aware of the duplex method before synchronizing to the cell. A radio frame of type 2 has a duration of 10 ms as its FDD equivalent. The TDD radio frame is also divided into 10 transmission time intervals of 1 ms duration called subframes. Furthermore, TDD subframes are split as well into two slots of 0.5 ms period.

TDD systems switch on one frequency between DL and UL transmission. Therefore, as described in Section 1.8.1, TDD needs defined switch points and guard intervals between UL and DL transmission.

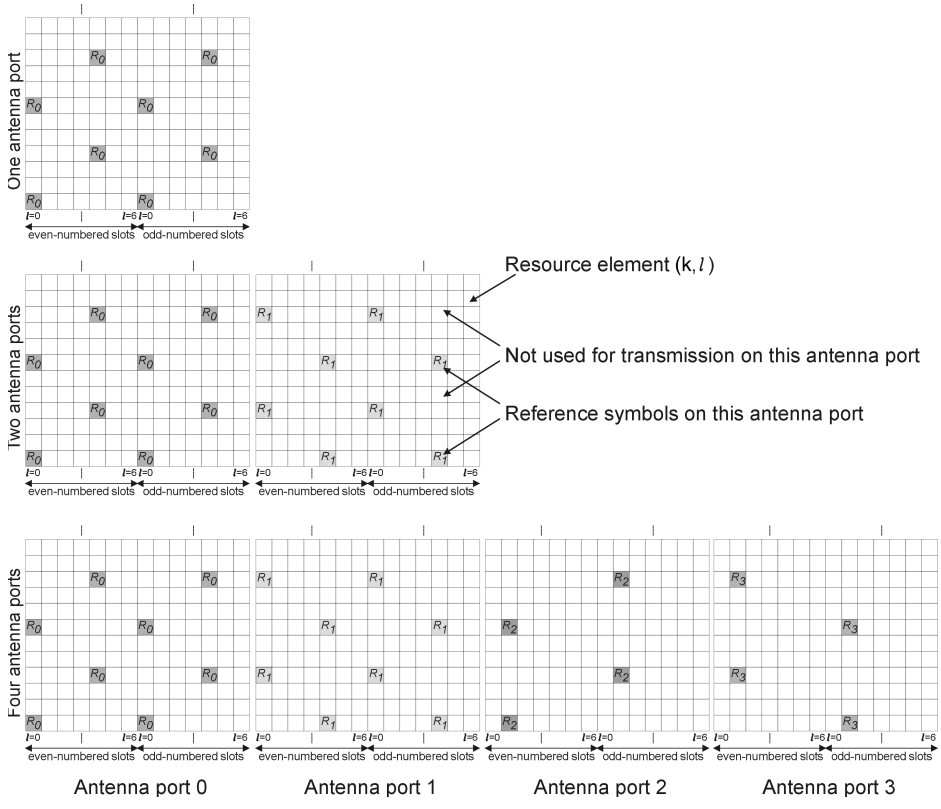


Figure 1.44 Mapping of downlink reference signals (normal cyclic prefix) (TS36.211). Reproduced with permission from © 3GPP™.

LTE defines two basic switch point interval durations of 5 and 10 ms. A switch point is a designated subframe divided into three zones which are already known from basic UMTS TDD: Downlink Pilot Time Slot (DwPTS), GP, and Uplink Pilot Time Slot (UpPTS). Other subframes are used for either UL or DL transmission. Operators can decide from UL–DL configurations which subframes are used as DL and UL depending on the UL and DL traffic mixture of a network. Seven different UL and DL structures are defined. The possible UL–DL configurations with the switch points and the subframe used for UL and DL transmission are given in Table 1.10.

Figure 1.45 shows a radio frame with frame structure type 2 used with TDD. This is an example with a 5 ms switch-point periodicity.

1.8.7 OFDM Scheduling on LTE DL

The eNB advises each UE when and on which resources to transmit its data or informs a UE where it should listen to receive data. The resources are defined by frequency and time units. This procedure

Table 1.10 Uplink–downlink configurations for TDD. Reproduced with permission from © 3GPP™

Uplink–downlink configuration	Downlink–uplink switch-point periodicity (ms)	Subframe number									
		0	1	2	3	4	5	6	7	8	9
0	5	D	S	U	U	U	D	S	U	U	U
1	5	D	S	U	U	D	D	S	U	U	D
2	5	D	S	U	D	D	D	S	U	D	D
3	10	D	S	U	U	U	D	D	D	D	D
4	10	D	S	U	U	D	D	D	D	D	D
5	10	D	S	U	D	D	D	D	D	D	D
6	5	D	S	U	U	U	D	S	U	U	D

S = Switching point.

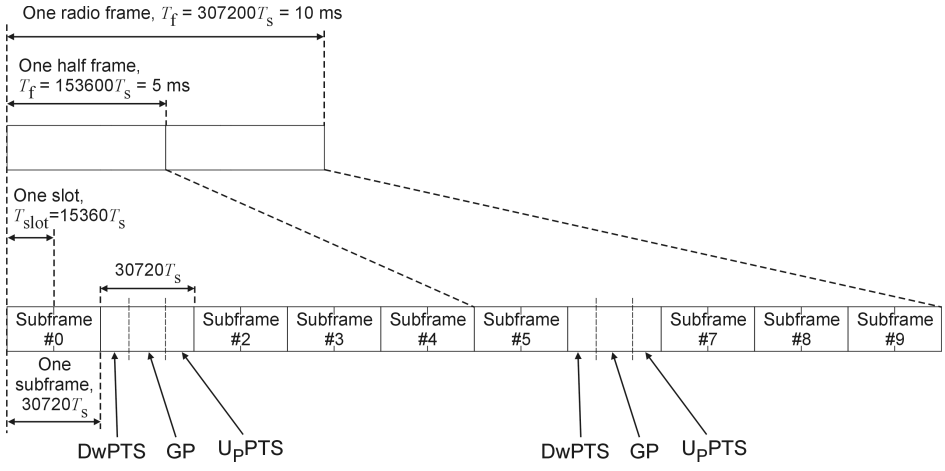


Figure 1.45 Frame structure type 2 used with TDD (for 5 ms switch-point periodicity) (TS36.211). Reproduced with permission from © 3GPP™.

of assigning system resource is called scheduling. The system resources are divided into units of RBs, as described in Section 1.8.5. Only integer numbers of RBs can be assigned to one user. Localized and distributed RB allocations are possible. Localized allocations assign adjacent RBs to one UE, distributed allocations distribute the scheduled RBs over the spectrum with gaps, for example, in order to achieve frequency diversity.

A new scheduling assignment is transmitted for each subframe, thus the scheduling period on the time axis is 1 ms. The DL scheduling information is transmitted in the PDCCH. The assignments on the frequency scale vary between one RB (minimal scheduled transmission) and the maximum number of available RBs in respect of the system bandwidth.

Generally, the LTE scheduling algorithm is not defined by the standard; it is a matter for the eNB vendors. This enables the base station vendors to differentiate between each other and use different optimization goals. Various parameters can be used as input for the scheduling decisions: channel quality of different users (measured or reported by the UE with the Channel Quality Indicator, CQI), QoS, congestion/resource situation, fairness, charging policies, and so on. Most schedulers aim to maximize the cell throughput under consideration of fairness metrics between cell edge users and users with very good channel conditions. Figure 1.46 shows a screenshot of a typical scheduling and cell resource allocation analysis tool. It gives insight into the scheduling process of the eNB and is able to evaluate the scheduler performance and the utilization of cell resources.

The CQI is reported in the UL direction and can be derived periodically or upon request by the eNB. It gives reception quality feedback to the scheduling algorithm in the eNB in order to schedule

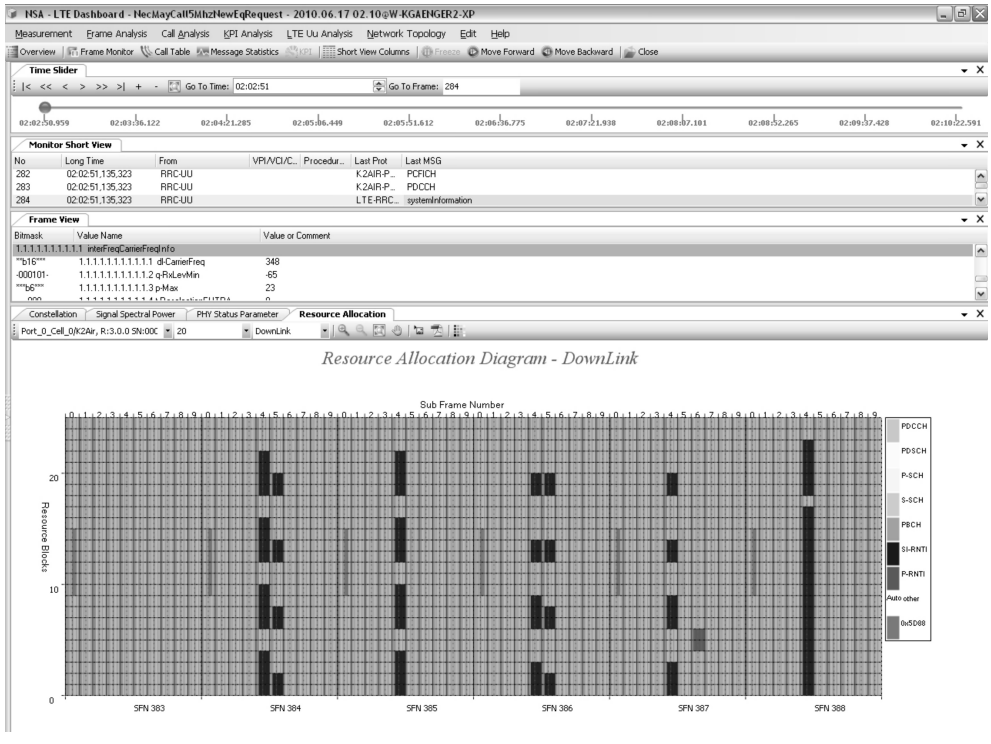


Figure 1.46 Scheduling and cell resource allocation analysis.

data on those frequency regions with the best possible reception characteristics. CQI is described further in Section 1.8.11.

The scheduling information is encoded as Downlink Control Information (DCI). The DCI is then mapped to REGs of the PDCCH. The length of the PDCCH can vary between one and three OFDM symbols depending on the load to be transmitted on the PDCCH. The number of used OFDM symbols is indicated in the PCFICH.

The DCI does not just transmit RB assignments and its assignment type, but also other information needed for the transmission or reception of data. This information is, for example, the Modulation and Coding Scheme (MCS), HARQ feedback information, or power control commands for UL transmission of the Physical Uplink Control Channel (PUCCH) or Physical Uplink Shared Channel (PUSCH) (see below).

The following DCI formats are defined and used for scheduling and UL Transmit Power Control (TPC) commands:

- **DCI format 0**: UL scheduling grant, see Section 1.8.9.
- **DCI format 1**: Single transport block (code word) scheduling assignment, for example, used for assigning resources to system information, paging, or random access. Further information: MCS, HARQ (New Data Indicator (NDI), redundancy version, HARQ process number), and TPC for PUCCH.
- **DCI format 1A**: Compact single transport block scheduling assignment. Further information: MCS, HARQ (NDI, redundancy version, HARQ process number), and TPC for PUCCH.
- **DCI format 1B**: A special DCI format for transmission mode 6 (MIMO closed loop rank 1 precoding). Further information: precoding vector, MCS, HARQ (NDI, redundancy version, HARQ process number), and TPC for PUCCH.
- **DCI format 1C**: Even more compact scheduling format as DCI 1A. For example, used for assigning resources to SIBs, paging, or RARs. This DCI is always transmitted using frequency diversity via distributed virtual resource block assignments using resource allocation type 2 (see below). This is done because channel feedback cannot be derived for such common information, as it is received by multiple users. The modulation is fixed to QPSK. Further information: MCS, HARQ (NDI, redundancy version, HARQ process number), and TPC for PUCCH.
- **DCI format 1D**: A special DCI format for transmission mode 5 (multi-user MIMO). Further information: MCS, HARQ (NDI, redundancy version, HARQ process number), power offset indicator if two UEs share power resources, and TPC for PUCCH.
- **DCI format 2**: Scheduling for transmission mode 4 (closed loop MIMO), multiple antenna port transmission operation, addressing multiple transport blocks (code words) to be transmitted on different antenna ports (layers). Further information: MCS for each transport block, HARQ (NDI, redundancy version, HARQ process number), number of transmission layers, precoding, and TPC for PUCCH.
- **DCI format 2A**: Used with transmission mode 3 (open loop MIMO using Cyclic Delay Diversity (CDD)), multiple antenna port transmission operation, addressing multiple transport blocks (code words) to be transmitted on different antenna ports (layers). Further information: MCS for each transport block, HARQ (NDI, redundancy version, HARQ process number), number of transmission layers, precoding, and TPC for PUCCH.
- **DCI format 3**: A 2-bit UL TPC command applying for PUSCH and PUCCH. Multiple users are addressed.
- **DCI format 3A**: A 1-bit UL TPC command applying for PUSCH and PUCCH. Multiple users are addressed.

The resource allocation assignments of the above DCI formats can use different resource allocation types. Table 1.11 maps the DCI formats to the allowed resource allocation types:

Table 1.11 Resource allocation types and the applying DCI formats TS36.213. Reproduced with permission from © 3GPP™

Resource allocation type	Applying DCI formats
Type 0	1, 2, 2A, and 2B
Type 1	1, 2, 2A, and 2B
Type 2	1A, 1B, 1C, and 1D

Table 1.12 Type 0 resource allocation RBG size vs. DL system bandwidth

System bandwidth N_{RB}^{DL}	RBG size (P)
$\leq$10	1
11–26	2
27–63	3
64–110	4

- **Resource allocation type 0**: With resource allocation type 0 a bit map is transmitted describing Resource Block Groups (RBGs). A RBG is a number of consecutive physical resource blocks (RBs). The number depends on the system bandwidth and has a range between one and four physical RBs. Table 1.12 maps the size of a RBG to the system bandwidth. The allocated RBGs do not have to be adjacent.
- **Resource allocation type 1**: The bit map transmitted with resource allocation type 1 makes use also of RBGs but can address single physical RBs by introducing additional flags. The number of RBGs is smaller than the ones used with resource allocation type 0, thus not reaching the complete bandwidth. The bit map addresses not whole RBGs, but a subset within each RBG which is pointed to by the bit map. A selection flag indicates the position within the RBG regions and a shift flag shows the position of the numbered RBGs within the system bandwidth as the number of RBGs does not address the complete system bandwidth: shift flag = 0 indicates that the RBGs start at the beginning of the system bandwidth leaving an unaddressable region at the end of the system bandwidth; shift flag = 1 indicates that the RBGs are shifted to the end of the system bandwidth leaving the unaddressable region at the beginning of the system bandwidth.
- **Resource allocation type 2**: This resource allocation type uses virtual RBs as scheduling units as described in Section 1.8.5. Two types of virtual RB scheduling assignments are used:
  - A localized type, where the allocated virtual RBs equal a number of consecutive physical RBs addressed with a starting RB and a number of adjacently assigned RBs. This information is encoded into an 11-bit Resource Indication Value (RIV).
  - A distributed type, where the addressed virtual RBs are distributed over the frequency with one or two gaps (depending on the system bandwidth) hopping at slot boundaries as described in Section 1.8.5. Virtually distributed RB assignments are always used with DCI format 1C. There is a 1-bit flag indicating whether virtual distributed or virtual localized RB assignment is used in the case of DCI formats 1A, 1B, and 1D.

Instead of addressing a UE with a PDCCH scheduling assignment (DCI) directly by adding a UE ID (e.g., a RNTI) to the DCI, the 16-bit CRC of the PDCCH message is scrambled with the RNTI, introducing common and UE-specific search spaces. This CRC scrambling saves additional resources

B24*	K2AIR-PHY (PDCCH)	Tektronix K2Air LTE PHY Data Message Header
B24*	1 PDCCH Message (Single UE Mode)	
B8	1.1 Common Message Header	
00000000	Protocol Version	0
----1101	Transport Channel Type	PDCCH/PUCCH Single UE mode
0100----	Physical Channel Type	PDCCH
b10*	System Frame Number	327
-----0--	Direction	Downlink
----1---	Radio Mode	FDD
---0----	Internal use	0
-00-----	Status	Original data
0-------	Reserved	0
b9	Physical Cell ID	0
----011-	UE ID/RNTI Type	C-RNTI
0111----	Subframe Number	7
B2	UE ID/RNTI Value	'a277'H
B16*	1.2 List of DCI for this UE	
B16*	1.2.1 DCI	
----0001	DCI Format	Format 1 - DL schedule
---1----	Last Format indicator	last DCI Format
--1-----	New Data Indicator DL 1	new data
01------	Transmit Power Control	+0 dB
---00000	Modulation Scheme Index DL 1	0
-00-----	Redundancy Version DL 1	0
0-------	Reserved	0
----0000	HARQ process number	0
-010----	Modulation Order DL 1	QPSK
0-------	Resource Allocation Type	Type 0
00000000	Reserved	0
B11*	1.2.1.1 List of allocated Downlink Resource Blocks	
-0000000	Resource Block ID	0
-0000001	Resource Block ID	1
-0000010	Resource Block ID	2
-0000011	Resource Block ID	3
-0000100	Resource Block ID	4
-0000101	Resource Block ID	5
-0010100	Resource Block ID	20
-0010101	Resource Block ID	21
-0010110	Resource Block ID	22
-0010111	Resource Block ID	23
-0011000	Resource Block ID	24
00000000	Padding	'00'H

Figure 1.47 Example PDCCH message of DCI format 1 (downlink scheduling assignment).

in DCIs, but increases slightly the chance of decoding a DCI for a different UE which is not intended to be addressed.

Figure 1.47 depicts an example PDCCH message of DCI format type 1 with all the transmitted information.

Some special applications require the transmission of small data chunks in equidistant periods of time. An example is a VoIP application. In order to minimize the signaling overhead in such cases, a mode Semi Persistent Scheduling (SRS) is introduced. SPS parameters are configured by the RRC layer, enabling the transmission of data on defined RBs in frequency and time without further scheduling on the PDCCH.

Battery energy saving is always an important topic with mobile handset systems. A potential scheduling assignment could be sent in each PDCCH which occurs every millisecond. Therefore, each attached UE would need to monitor the PDCCH each millisecond for scheduling information. The DRX mode enables the UE just to listen to defined subframes for scheduling assignments and turn off its receiver in between, in order to save battery consumption. Short and long DRX cycle periods are defined. The DRX parameters are set by MAC and RRC. Figure 1.48 depicts a DRX cycle.

1.8.8 SC-FDMA Principles and Modulation

The OFDM transmission scheme shows robustness against multipath fading and is especially useful for mobile communication systems due to various reasons. An example is the complexity of the receiver where fairly simple and channel estimation/equalization is done in the frequency domain. Why is another transmission scheme selected for the LTE UL? A major disadvantage of OFDM systems is

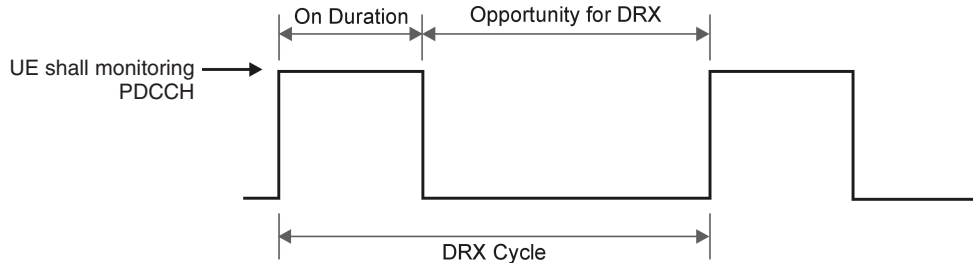


Figure 1.48 DRX cycle. Reproduced with permission from © 3GPP™.

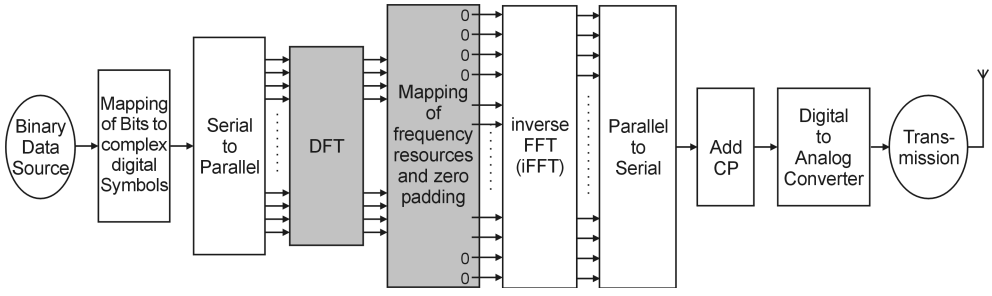


Figure 1.49 Block diagram of SC-FDMA transmitter with localized mapping to frequency resources.

that the time domain signal which is amplified and transmitted shows a large dynamic range after modulating symbols on subcarriers and transformation to a time signal. This leads to a high Peak-to-Average Power Ratio (PARP) of the signal, which should be avoided for battery-powered handsets, which underlies a limit on the budget to justify the business case. The linear transmission of such a signal needs a highly complex RF amplifier for the handsets in order not to run into the nonlinear region of the transmitter. Additionally, the power consumption is larger compared to a transmitter running a smaller linear dynamic range. The PAPR even increases with a wider OFDM bandwidth for a larger number of modulated subcarriers. This results in another transmission scheme for the UL: Single Carrier FDMA (SC-FDMA).

Actually SC-FDMA is very similar to OFDMA but shows a better PAPR, leading to a longer battery lifetime and a cost-effective RF amplifier design. Figure 1.49 illustrates the components of a SC-FDMA transmitter system with its block entities. Highlighted in the figure are the main differences from a regular OFDM system. The main difference is the Discrete Fourier Transform (DFT) in the transmitter and the inverse DFT (iDFT) in the receiver, respectively. Thus, SC-FDMA is sometimes called DFT-spread-OFDM. Due to this difference, we can picture the information to be transmitted as modulated (bits mapped to two-dimensional QAM symbols with an I and Q component) to a time domain signal instead of modulating subcarriers of a frequency domain signal. The output of the DFT can be interpreted as a spectrum of the previously modulated data symbols. This spectrum has the characteristic of consecutive modulated subcarriers; it has therefore no scattered spectral distribution. Thus, it has the inherent behavior of localized RE usage as described in Section 1.8.5.

This localized spectrum is now mapped to the consecutive frequency REs which are specified in the UL scheduling grant, as only localized frequency resource assignments are allowed with UL transmission, which refers to the intrinsic signal characteristic of DFT-spread-OFDM. The rest of the spectrum for the full system bandwidth is filled with zeros. This zero patched spectrum is fed to

an iFFT unit transforming a full system-wide spectrum “back” to the time domain for transmission. Figure 1.49 shows this mapping of the DFT symbols to the full iFFT width by adding zeros to frequency positions at the block in the center. The zero patched frequency areas are not used by this user and could be assigned to other users transmitting in the same time slot.

As for the future, a current research item is to overcome the lack of a high PAPR of OFDM signals in such a way that a digital reverse distorted signal is added to the signal which is to be transmitted. The nonlinear distortion is known for a given RF amplifier. Therefore, it is possible to pre-calculate the distortion applied to the transmitted signal. This distortion is inverted and joined to the signal to such a degree that the RF amplifier distortion eliminates the inverted signal again.

1.8.9 Scheduling on LTE UL

The LTE UL scheduling is very similar to the DL scheduling described in Section 1.8.7, although the UL scheduler is a distinct entity. This section describes the difference from the DL scheduling only.

UL scheduling grants are indicated to the UE by transmitting all relevant UL scheduling information within the PDCCH. This is done by using a dedicated DCI type, DCI 0. Each UE has to monitor the PDCCH in every subframe for DCI types 0 scrambled with their RNTI (for a message example see Figure 1.50). This does not apply for the case when power saving mode DRX is enabled, which switches off the UE’s receiver periodically. UL resources are allocated without a designated PDCCH UL grant in the case of SPS (see Section 1.8.7) or for non-adaptive HARQ retransmissions. A non-adaptive HARQ retransmission is triggered by the transmission of a Negative Acknowledgment (NACK) by the UE.

In the UL only localized scheduling is allowed, which means that an integer number of consecutive RBs is allocated to one UE. Furthermore, there is only one scheduling process per UE, thus there is not a dedicated scheduling process per radio bearer.

The UE feeds the UL scheduler with CQI, Buffer Status Reports (BSRs), ACKs/NACKs, and Scheduling Requests (SRs). BSRs indicate the fill level status of the current transmit buffer. This buffer status is reported in bins, quantizing the fill level in bytes. Figure 1.51 shows an example of a MAC BSR message.

BITMASK	ID Name	Comment or Value
B65*	LTE-RLC/MAC (MAC-PDU (UL))	3GPP LTE-RLC/MAC Rel.8 (MAC TS 36.321 V8.5.0, 2009-03, RLC TS 36.322 V8.5.0, 2009-03)
B65*	1 MAC PDU (Uplink)	
B4	1.1 MAC Header Part	
00111101	1.1.1 MAC PDU Subheader	
00------	Reserved	0
--1-----	Extension field	Another MAC PDU subheader follows
---11101	LCID-UP	Short BSR
B2	1.1.2 MAC PDU Subheader	
00------	Reserved	0
--1-----	Extension field	Another MAC PDU subheader follows
---00010	LCID-UP	Logical Channel 2
0-------	Format field	7-Bits Lengthfield
-0111000	SDU Length	56
00011111	1.1.3 MAC PDU Subheader	
00------	Reserved	0
--0-----	Extension field	Last MAC PDU subheader
---11111	LCID-UP	Padding
B61*	1.2 MAC Payload Part	
00000111	1.2.1 MAC Control Short BSR	
00------	Logical Channel Group ID	0
--000111	Buffer Size	22 < BS <= 26
	Logical Channel ID	2
B56*	1.2.2 RLC Data PDU (acknowledged mode)	
1-------	D/C	Data
-0------	RF	AMD PDU
--1-----	P	Status report is requested
---00---	FI	0
	Framing Info	First byte is first of SDU, Last byte is last...
-----1--	E	A set of E & LI field follows on next octet
b10*	SN	0
b12*	1.2.2.1 E LI Set	
0-------	E	Data field follows on next octet
b11*	LI	26
----0000	Padding	0
B26*	1.2.2.2 RLC Data with LI	
B26*	Data with LI	00 48 02 41 00 41 e6 86 86 06 06 06 06 06 06...
B26*	1.2.2.3 RLC Data	
B26*	Data	01 48 02 41 00 41 e6 86 86 06 06 06 06 06 06...
B4	1.2.3 MAC Padding	
B4	macPad	'00000000'H

Figure 1.50 Example PDCCH message of DCI format 0 (uplink scheduling grant).

BITMASK	ID Name	Comment or Value
B65*	LTE-RLC/MAC (MAC-PDU (UL))	3GPP LTE-RLC/MAC Rel.8 (MAC TS 36.321 V8.5.0, 2009-03, RLC TS 36.322 V8.5.0, 2009-03)
B65*	1 MAC PDU (Uplink)	
B4	1.1 MAC Header Part	
00111101	1.1.1 MAC PDU Subheader	
00------	Reserved	0
--1-----	Extension field	Another MAC PDU subheader follows
---11101	LCID-UP	Short BSR
B2	1.1.2 MAC PDU Subheader	
00------	Reserved	0
--1-----	Extension field	Another MAC PDU subheader follows
---00010	LCID-UP	Logical Channel 2
0-------	Format field	7-Bits Lengthfield
-0111000	SDU Length	56
00011111	1.1.3 MAC PDU Subheader	
00------	Reserved	0
--0-----	Extension field	Last MAC PDU subheader
---11111	LCID-UP	Padding
B61*	1.2 MAC Payload Part	
00000111	1.2.1 MAC Control Short BSR	
00------	Logical Channel Group ID	0
--000111	Buffer Size	22 < BS <= 26
	Logical Channel ID	2
B56*	1.2.2 RLC Data PDU (acknowledged mode)	
1-------	D/C	Data
-0------	RF	AMD PDU
--1-----	P	Status report is requested
---00---	FI	0
	Framing Info	First byte is first of SDU, Last byte is last...
-----1--	E	A set of E & LI field follows on next octet
b10*	SN	0
b12*	1.2.2.1 E LI Set	
0-------	E	Data field follows on next octet
b11*	LI	26
----0000	Padding	0
B26*	1.2.2.2 RLC Data with LI	
B26*	Data with LI	00 48 02 41 00 41 e6 86 86 06 06 06 06 06 06...
B26*	1.2.2.3 RLC Data	
B26*	Data	01 48 02 41 00 41 e6 86 86 06 06 06 06 06 06...
B4	1.2.3 MAC Padding	
B4	macPad	'00000000'H

Figure 1.51 Example MAC Buffer Status Report (BSR) message.

LTE trial studies show that there are various cases of scheduled empty UL grants. This happens when the eNB assigns UL resources to a UE and the designated UE does not use those UL resources for an UL transmission. Operators should minimize such empty scheduled UL resource in order to optimize the usage of UL radio resources.

1.8.10 Uplink Slot Structure

The UL slot structure is similar to the DL slot structure. Differences are mainly due to simplifications of reference symbols, robustness, and physical UL channel multiplexing. A radio frame lasts 10 ms and is divided into 10 subframes with two slots of 0.5 ms duration as a DL radio frame is split into subframes and slots. Figure 1.52 shows an UL radio frame with its subframe and slot structure. An UL RB has 12 subcarriers on the frequency axis and on the time domain it has, seven SC-FDMA symbols per slot when normal CP is used, and six SC-FDMA symbols when extended CP is used (see Figure 1.53).

UL synchronization signals are not used because all UL signals from UEs transmitting within the cell are time aligned at the eNB with an UL timing control procedure. The eNB signals a Timing Advance (TA) command to each UE to track the UL alignment. Timing varies due to the different special distribution of UEs within a cell region. Signals are delayed because of the propagation delay. Firstly, during the random access procedure a total timing offset to the UE is transmitted. After this there is a control loop just tracking and signaling differential timing offsets in steps of 0.52 µs ($16 \times T_s$).

The PRACH always uses six consecutive RBs on the frequency axis and is time-wise one subframe wide. Which six RBs are used is variable and set in SIB type 2. The PRACH configuration index is signaled in SIB type 2 as well, which defines the subframes which carry the PRACH's six RBs. This subframe configuration applies for either even or any radio frame. There are 64 possible PRACH configuration index permutations.

Resources at the upper and lower edges of the system bandwidth are used to carry the PUCCH. The frequency resources in between the PUCCH bands are designated to PUSCH transmission.

UL reference signals are used for UL channel estimation. DL reference signals are spread over frequency and time as single REs, which leads to a two-dimensional spheric channel estimation. UL

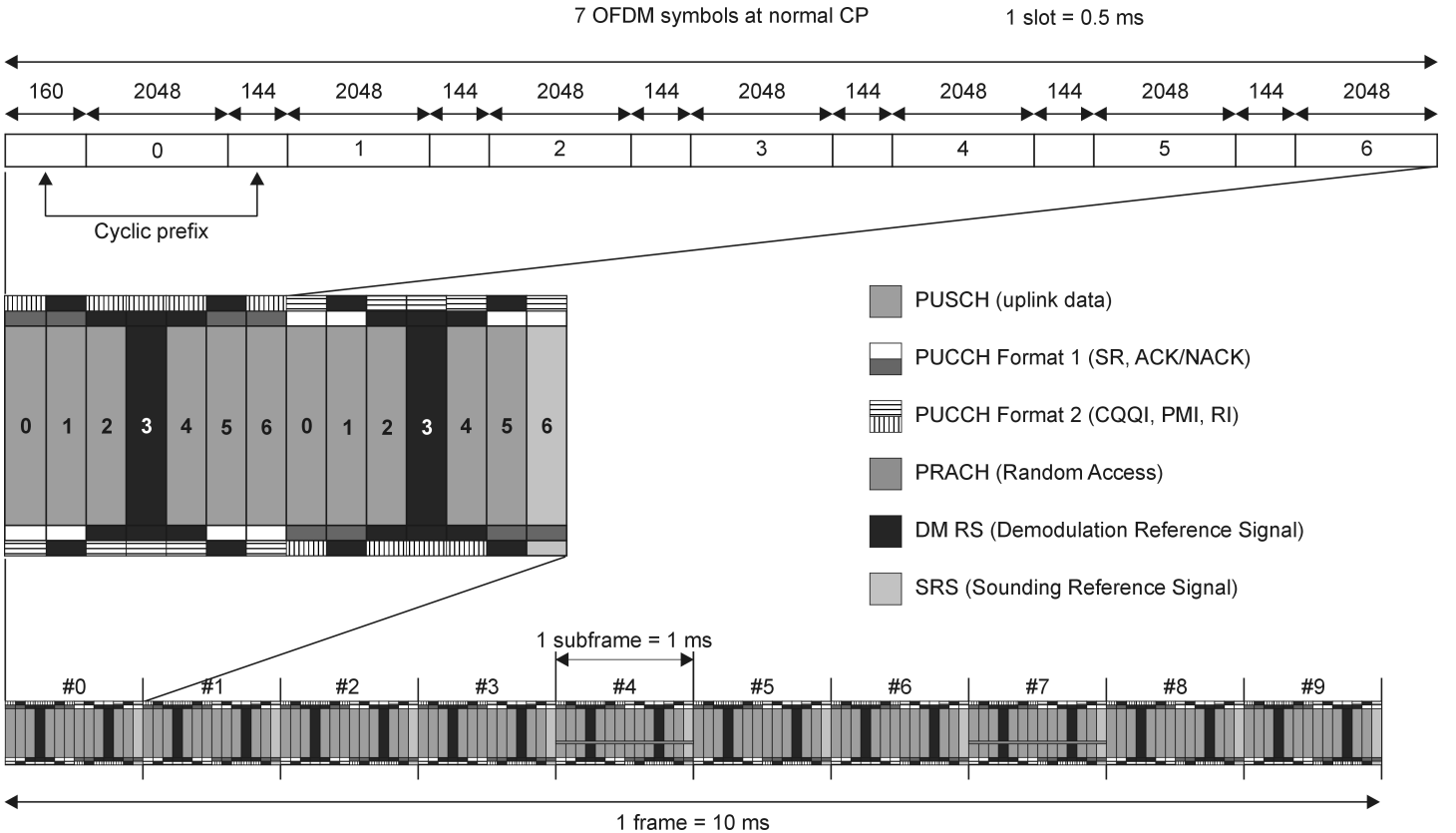


Figure 1.52 Uplink radio frame and subframe with two slots including PUSCH, PUCCH, PRACH, DMRS, and SRS. Reproduced with permission from Nomor.

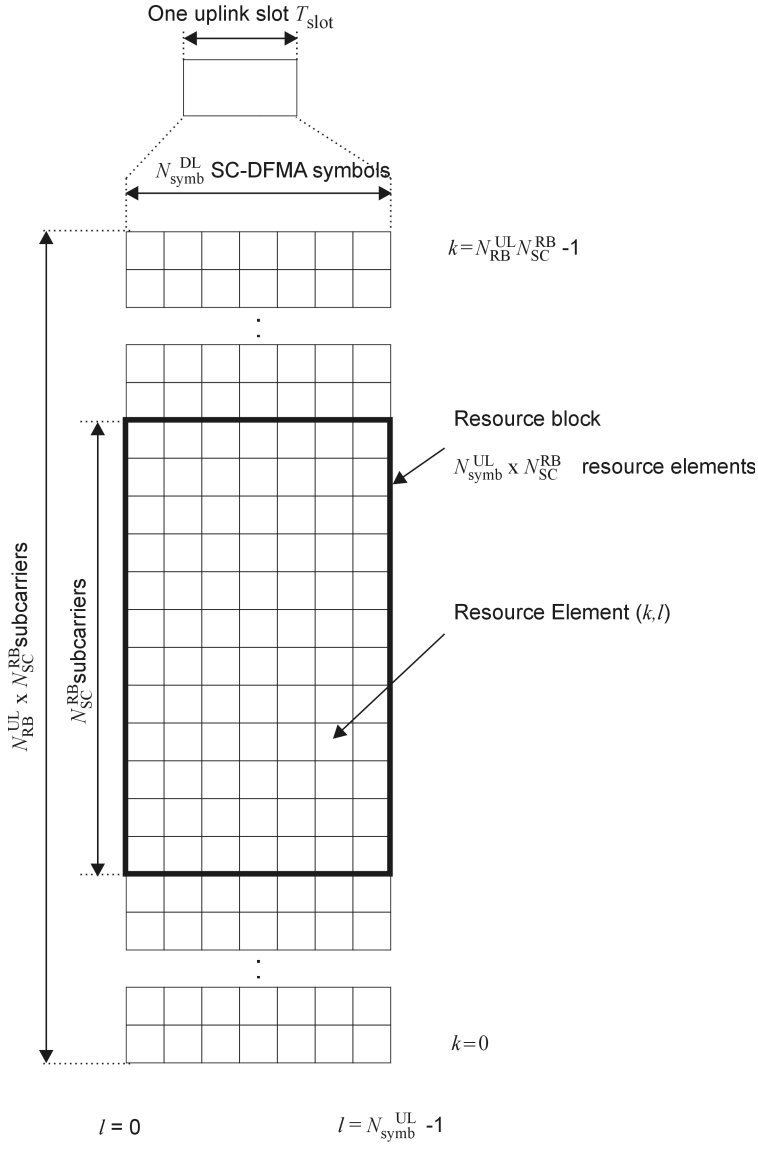


Figure 1.53 Uplink resource grid showing on UL RB. Reproduced with permission from © 3GPP™.

reference signals are similar to TDMA pilots in the middle of each time slot. LTE defines reference signals in the middle of each slot (on the fourth OFDM symbol assuming normal CP duration) and spanning via the complete allocated frequency range of each UE.

The eNB can instruct UEs to transmit special reference signals over the complete system bandwidth, or parts of it, independently of UL data transmission either on PUSCH or PUCCH. These reference signals are called Sounding Reference Signals (SRSs). SRSs are used to estimate UL channel quality of a wider frequency range in order to optimize frequency-selective UL scheduling.

Figure 1.52 depicts, in addition to the radio frame, a zoomed UL subframe with a PUCCH and PUSCH example configuration with UL demodulation reference symbols (DMRS) and SRS symbols.

1.8.11 Link Adaptation in LTE

Mobile wireless reception conditions vary greatly over frequency and time as described in Section 1.8. In order to cope with these circumstances and guarantee best possible QoS, a procedure is implemented known as Adaptive Modulation and Coding (AMC). AMC controls and changes transmission parameters to achieve a defined Transport Block Error Rate (BLER) of below 10%, in order to keep retransmissions in a suitable range. This is done by adapting the modulation scheme, in LTE on the shared channels between QPSK and 64QAM, and the Forward Error Correction (FEC) coding rate.

Different modulation schemes make the bit detection more robust against noise and other distortion caused by the wireless channel. Figure 1.54 shows the applied modulation scheme for the LTE shared channels. Most robust transmission is achieved by mapping just 2 bits to each modulation symbol as seen with QPSK, resulting in four stages. A large distance between modulation points as seen with QPSK allows a higher probability of the correct decision at the receiver even with noisy reception conditions. Both 16QAM and 64QAM map 4 and 6 bits respectively to one modulation symbol used with better wireless channel conditions to achieve a higher data throughput. It is to find the best compromise between the modulation scheme and code rate for a given channel quality. LTE defines a list of MCS combinations and just signals an MCS index.

The data modulated with the different modulation schemes to subcarriers needs to be protected against transmission errors. LTE defines a turbo de-/encoder with trellis termination of a native code rate of one-third. The turbo coder adds redundancy bits to the data, which makes it possible to correct some bit errors. The code rate is a fraction of source data rate to resulting protected data rate; thus, a code rate of one-third encodes 1 bit into 3 bits. Other code rates are needed in order to optimize the trade-off between protection and efficiency. This is done by puncturing the native coded bit stream to a higher (less protection) code rate by deterministically leaving out coded bits, or by deterministically repeating coded bits if a smaller code rate is desired (more protection).

Additionally, one parameter being controlled is the UL transmit power. UL power control is implemented to deal with the near–far effect. Figure 1.55 shows an UL scenario with a near–far effect compared to a DL scenario without power differences between user signals as they are equally attenuated because the mix of the signal is transmitted from one position (eNB). This occurs when a user is close to the base station (near) and another user is far away from the base station, introducing a higher power path loss which leads to a lower receive power of the signal of the cell edge user. All

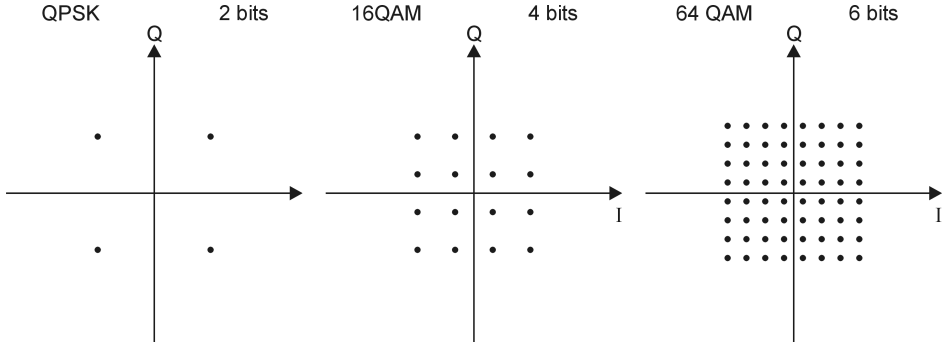


Figure 1.54 Different QAM schemes used with LTE and the number of bits mapped to each scheme.

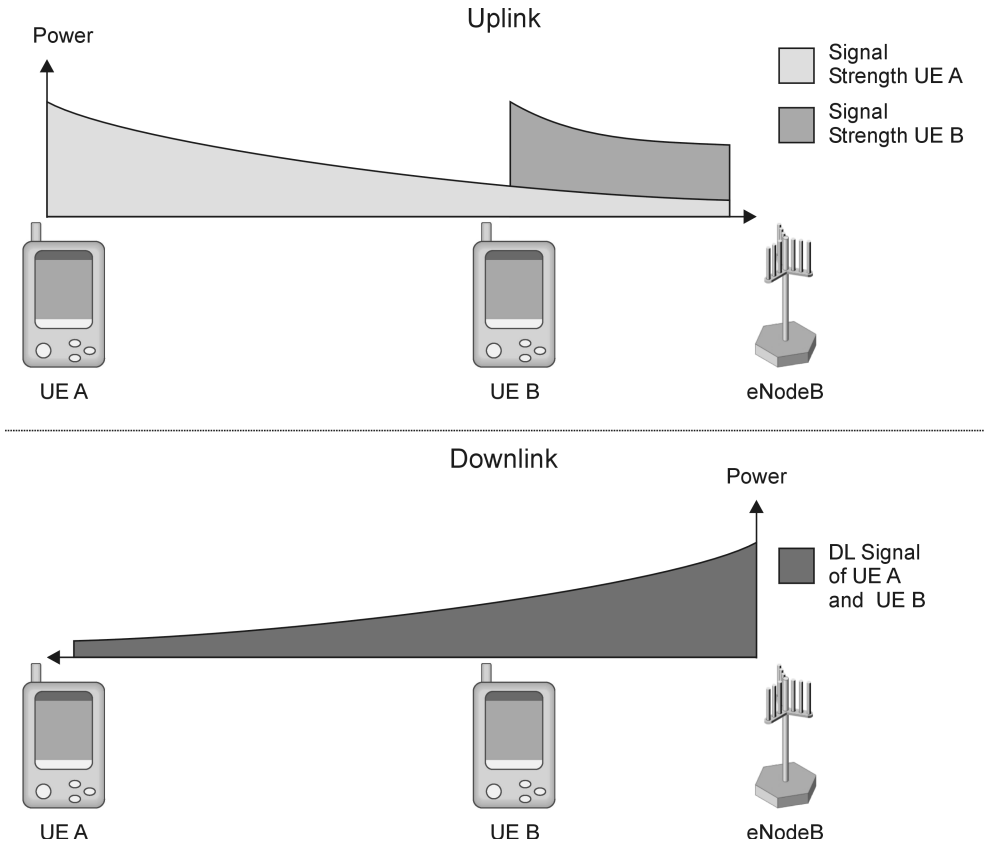


Figure 1.55 Near–far effect occurring in uplink direction, compared to equal signal strength reception in downlink.

UL receive signals should have equal power in order to have the same analog-to-digital converter saturation of each signal to reduce the quantization noise of users with low received signals, reducing inter-subcarrier interference between the users. This happens with imperfect UL synchronization within real-life scenarios.

UL TPC commands are sent via designated DCI formats 3 and 3A. DCI 3 and 3A are differential power control commands for PUCCH and PUSCH transmission in steps of decibels. DCI 3 is a 2-bit assignment as opposed to DCI 3A which is a single bit command. These dedicated DCIs with TPC commands are only used when there is no data to be transmitted to the UE; otherwise, the TPC command is transmitted embedded in other control information on the PDCCH for this UE. An initial 3-bit TPC command is embedded in the RAR message, see Section 1.8.16. The different TPC commands are listed in Tables 1.13 and 1.14.

UEs report their received channel quality to the eNB by transmitting a CQI value (see also Section 1.8.7). The CQI value represents either a wideband receive quality as a scalar or a more detailed report about frequency sections (sub-bands) as a vector. CQI reports are transmitted periodically or aperiodically configured by higher layers. Sub-band CQI reports indicate the receive quality of each sub-band relative to the wideband average with four steps: worse, equal, better, and much

Table 1.13 Mapping of TPC command field in DCI format 1A/1B/1D/1/2A/2/3 to δ_{PUCCH} values. Reproduced with permission from © 3GPP™

TPC command field in DCI format 1A/1B/1D/1/2A/2/3	δ_{PUCCH} (dB)
0	−1
1	0
2	1
3	3

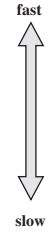
Table 1.14 Mapping of TPC command field in DCI format 3A to δ_{PUCCH} values. Reproduced with permission from © 3GPP™

TPC command field in DCI format 3A	δ_{PUCCH}(dB)
0	−1
1	1

better. The UE reports the best M sub-bands compared to the average channel quality with the best M method as depicted in Figure 1.56.

The UE should derive a MCS scheme from the above measurement information, which is indexing 1 MCS out of 16 to suit the target BLER of below 10%. This enables differentiation between high- and low-cost handsets which use more or less expensive RF hardware and/or a more sophisticated IQ signal processing engine.

Recapitulating, LTE link adaptation uses various stacked link adaptation techniques, securing transmission, or in order to make it more effective using different control loop delays regarding the process's dimension. The following items summarize the LTE link adaptation functions with their responsiveness:



- **Adaptive frequency-selective scheduling**: Assign frequency resource to UEs on a 1 ms basis, which provides each UE with the individual best reception quality.
- **AMC**: Obtain the most efficient modulation and FEC code rate in order to balance retransmissions vs. maximization of throughput.
- **HARQ**: Multiple retransmission process using prior transmission to increase the correct decoding probability.
- **TPC**: Provides UL power control in order to minimize multiple user interference.

1.8.12 Physical Channels in LTE

As indicated in the above sections, LTE uses a completely new transmission scheme and physical layer design compared to WCDMA, resulting in an entirely new physical channel layout. Main user data, both control plane and user plane, is transmitted via shared channel architecture. Physical control channels control physical layer procedures only.

Physical DL channels and signals are listed below. Physical channels carry user-relevant information and physical signals do not carry user-specific information, just the SSS.

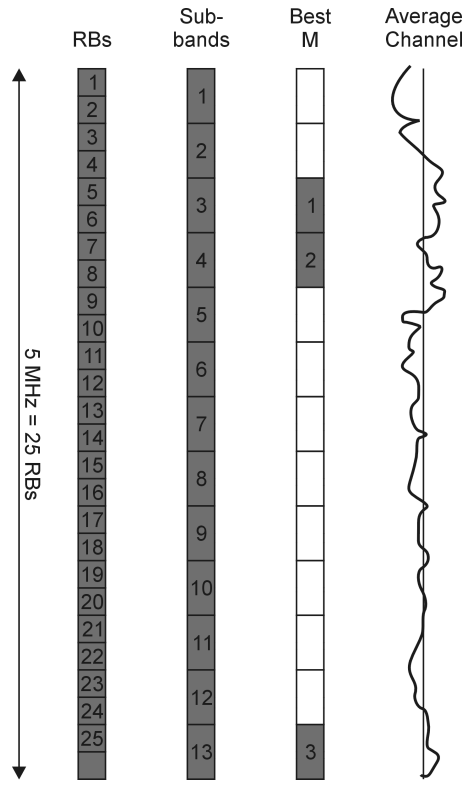


Figure 1.56 CQI illustration with sub-bands and best M reporting. Reproduced with permission from Nomor.

Physical DL channels:

- Physical Downlink Shared Channel (PDSCH).
- Physical Broadcast Channel (PBCH).
- Physical Multicast Channel (PMCH).
- Physical Control Format Indicator Channel (PCFICH).
- Physical Downlink Control Channel (PDCCH).
- Physical HARQ Indicator Channel (PHICH).

DL signals:

- Reference signals.
- Synchronization signals:
  - Primary Synchronization Signal (PSS).
  - Secondary Synchronization Signal (SSS).

1.8.12.1 PDSCH

As LTE relies fundamentally on shared channel architecture, the PDSCH carries all data in the DL direction to the UEs within a cell. RBs with their REs are modulated with user data (MAC PDUs,

Packet Data Units) as described in the above sections. The PDSCH bears both control plane (in-band signaling) and user plane data, which is multiplexed on logical channels on the DL-SCH as described in Section 1.8.14. Data is transmitted using adaptive modulation schemes of QPSK, 16QAM, or 64QAM.

UE-specific RRC messages are transmitted with the PDSCH together with user plane packets, and also with paging and system broadcast information (SIBs).

The different Transmission Modes (TMs) such as, for example, multiple antenna transmission or single antenna transmission, apply for the PDSCH only. Different TMs can be used dynamically between UEs signaled within the rrcConnectionSetup message.

Defined TM:

- **TM 1**: Single antenna transmission.
- **TM 2**: Transmit diversity.
- **TM 3**: Open loop spatial multiplexing (MIMO) using Cyclic Delay Diversity (CDD). The signal is transmitted on another antenna with a cyclic delay, in order to increase the multipath reception which leads to a MIMO gain.
- **TM 4**: Closed loop spatial multiplexing (MIMO).
- **TM 5**: Multi-user MIMO (or "virtual" MIMO).
- **TM 6**: Closed loop rank 1 precoding.
- **TM 7**: Beamforming (Space Division Multiple Access (SDMA)) with UE-specific reference symbols.

Each transport block transmitted on the PDSCH is transmitted with a 24-bit checksum for error detection.

1.8.12.2 PBCH

The PBCH carries the Master Information Block (MIB), which is transmitted logically in an interval of 40 ms. FEC is protecting the MIB in such a way that four equal-sized blocks are derived. It is possible to decode each block individually and retrieve all the information in the MIB. Each block is transmitted in the PBCH resources in every radio frame (see Figure 1.57), thus a MIB is decodable every 10 ms.

Information being transmitted is mainly the system bandwidth in RBs. An example of a PBCH for 5 MHz bandwidth with 25 RBs is shown in Figure 1.58.

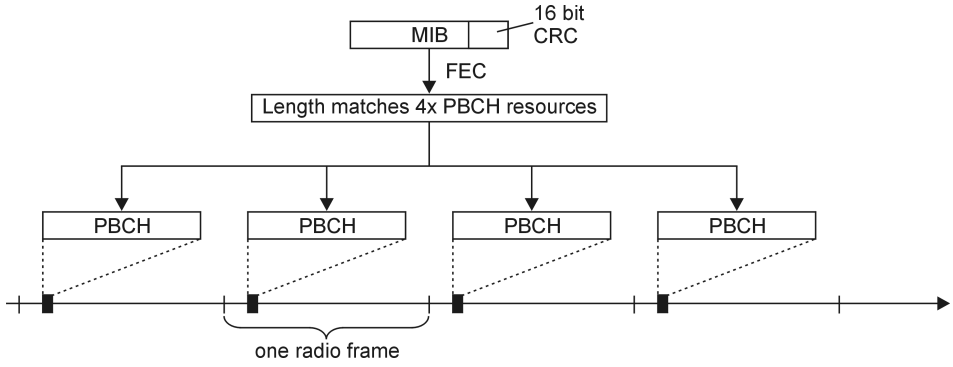


Figure 1.57 Master information block encoding and mapping to four DL radio frames.

B3	LTE-RLC/MAC (MAC-TM-PDU (DL))	3GPP LTE-RLC/MAC Rel.8 (MAC TS 36.321 V8.5.0, 2009
B3	1 MAC PDU (Transparent Content Downlink)	
B3	MAC Transparent Data	49 80 00
B3	LTE-RRC_BCCH_BCH (bCCH-BCH-Message)	RRC (BCCH to BCH) 3GPP TS 36.331 V8.5.0 (2009-03)
B3	bCCH-BCH-Message	
B3	1 bCCH-BCH-Message	
B3	1.1 message	
010-----	1.1.1 dl-Bandwidth	n25
---010--	1.1.2 phich-Config	
---0----	1.1.2.1 phich-Duration	normal
----10--	1.1.2.2 phich-Resource	one
b8	1.1.3 systemFrameNumber	'60'H
b10*	1.1.4 spare	'0000000000'B

Figure 1.58 Example of a MIB (PBCH) broadcast channel message.

As illustrated in Figures 1.60 and 1.61 below, the PBCH is located in each first subframe of every radio frame. It allocates the six center RBs (72 REs) regardless of the system bandwidth of the first four OFDM symbols in the second slot.

1.8.12.3 PMCH

Multicast transmission (e.g., MBMS) is a feature of later LTE releases, although it is necessary to define all physical channels already at this stage, in order to define a backward-compatible physical layer. The PMCH is transmitted on the fourth antenna port only with designated reference symbols. This channel is basically similar to the PDSCH, but designed for a multicell reception.

1.8.12.4 PCFICH

The PCFICH is transmitted in the first OFDM symbol of each subframe and indicates the number of OFDM symbols used for the PDCCH. Control format indicator values run from 1 to 4, but only a maximum of three OFDM symbols is defined by the first release of LTE, reserving value 4 for future use. Because it is needed to correctly decode the PCFICH, the information carried is very well protected. Values 1–4 are encoded with a 32-bit pattern and modulated with QPSK to 16 subcarrier (REs), as 2 bits can be mapped to a QPSK symbol. Those 16 REs are mapped to four REGs. The REGs are not adjacent in order to gain frequency diversity. Figure 1.59 shows an example mapping of the PDCFICH to the first OFDM symbol of the PDCCH. The position of the PCFICH information is shifted and scrambled by the physical c-ID, in order to protect it against intercell interference. Figure 1.59 shows examples for three different c-ID ranges.

1.8.12.5 PDCCH

The PDCCH is needed to transport DCIs. DCIs carry information on scheduling assignments for the DL and scheduling grants for the UL as described in Sections 1.8.7 and 1.8.9. Various DCI formats are defined for scheduling tasks, and DCI 3 and 3A (Section 1.8.11) for UL TPC. This channel is mapped to the first one to three OFDM symbols of each subframe as signaled by the PCFICH.

Figure 1.60 depicts a detailed example mapping of the PDCCH in which each square represents on RE (one subcarrier within an OFDM symbol). Each column is one OFDM symbol with respect to time (horizontal) and frequency (vertical). White areas (REs) are used for the user data transmission (PDSCH). Black REs are fixed and allocated for DL reference signals (see Figure 1.44 for detailed illustrations of antenna mappings in the case of multiple antenna ports).

The PDCCH is transmitted in the DwPTS subframe with TDD.

In Sections 1.8.7 and 1.8.9 example PDCCH messages are described for DL scheduling and UL scheduling assignments respectively.

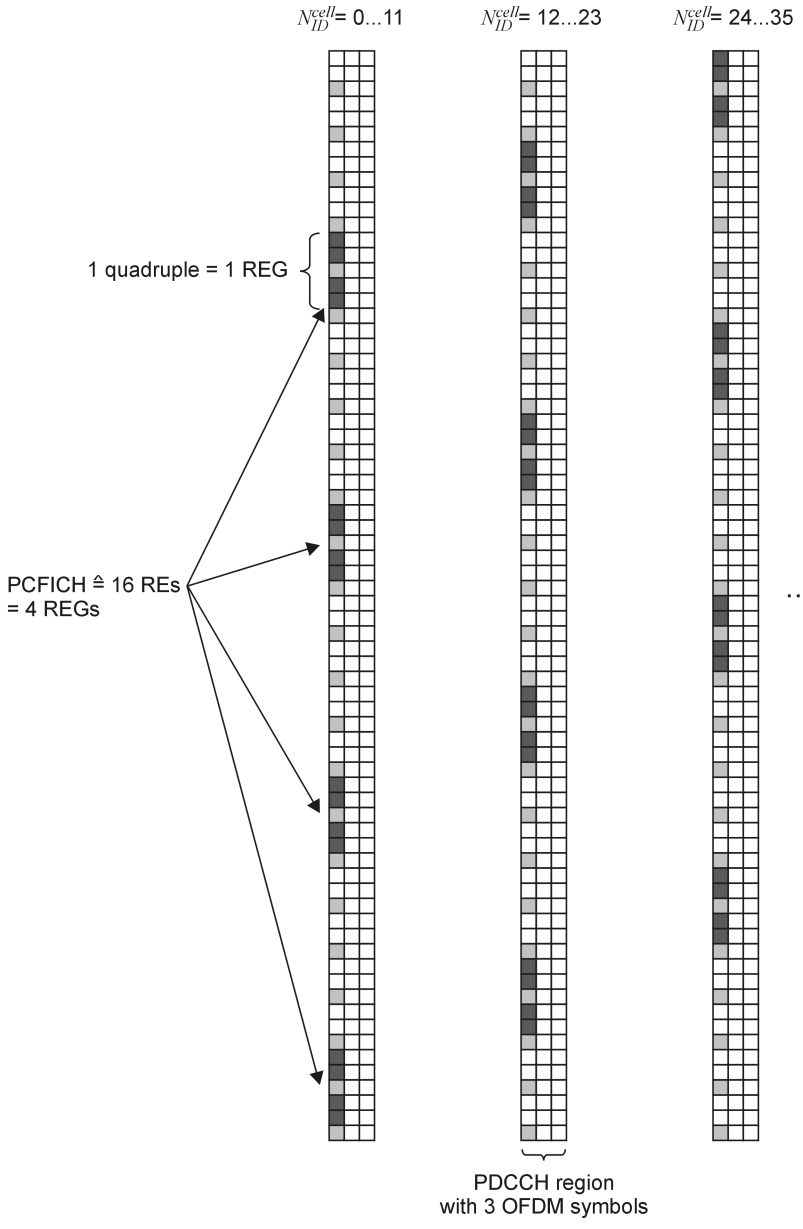


Figure 1.59 Mapping examples of PCFICH into resource element groups (always within the first OFDM symbol of a subframe) within the PDCCH area. Reproduced with permission from Nomor.

UE-specific DCI is addressed to UEs implicitly by scrambling the CRC to save signaling resources. The DCI can be located in various positions, thus UEs have to blind-decode and "search" for their designated information. Twelve common search spaces and 32 UE-specific search spaces are defined, resulting in a worst case of 44 decoding attempts.

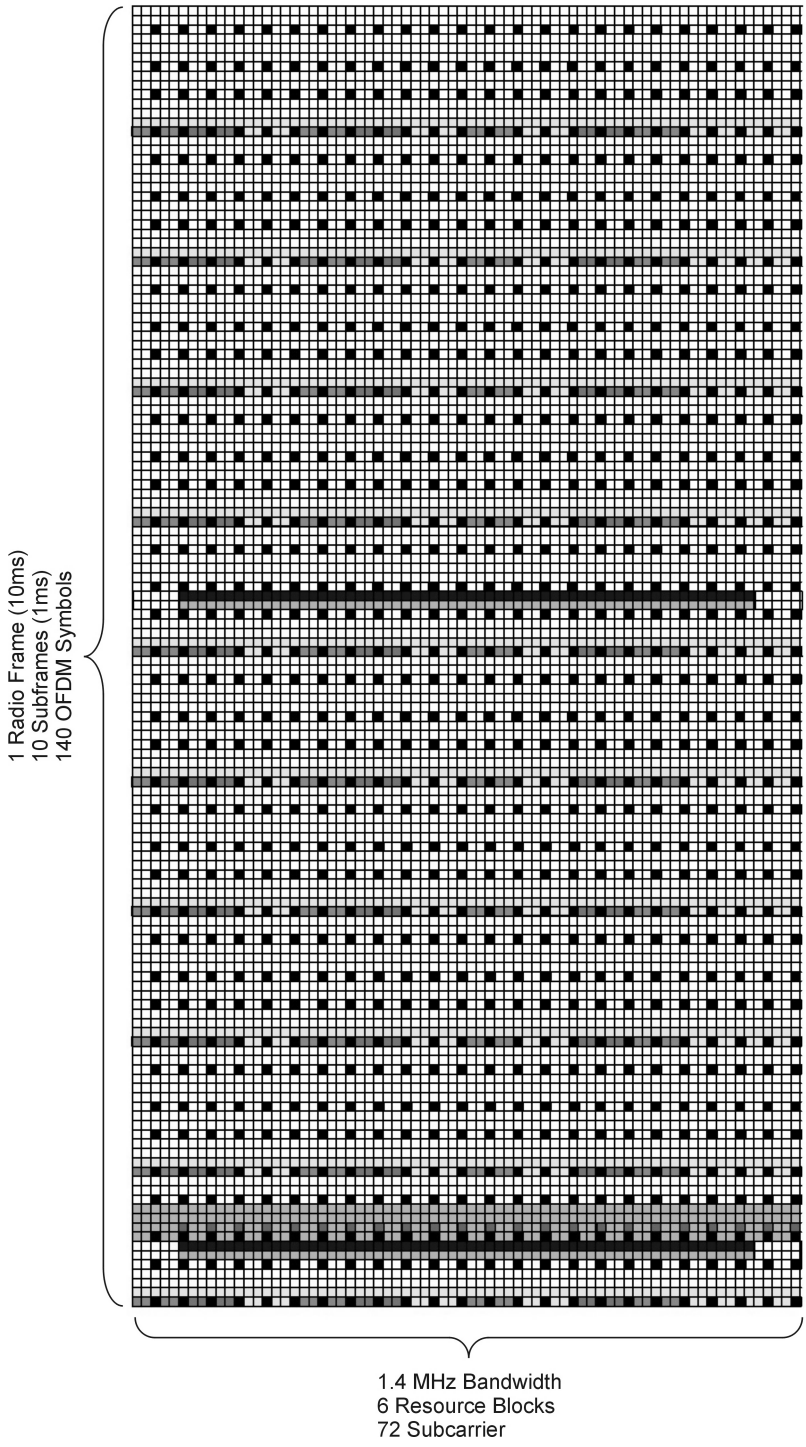


Figure 1.60 Detailed illustration of one DL radio frame for a 1.4 MHz bandwidth example with mappings of all DL physical channels and signals. Reproduced with permission from Nomor.

Table 1.15 Supported PDCCH formats with different FEC protection. Reproduced with permission from © 3GPP™

PDCCH format	Number of CCEs	Number of resource element groups	Number of PDCCH bits
0	1	9	72
1	2	18	144
2	4	36	288
3	8	72	576

Different PDCCH formats are specified which use different FEC protection code rates in order to achieve higher protection, for example, for cell edge users with poor reception conditions (see Table 1.15).

1.8.12.6 PHICH

The PHICH carries HARQ feedback information in the DL to the UEs. In other words, the ACK or NACK of a previous UL transmission is signaled to the sending UE via the PHICH. This feedback information (1 bit) is repeated three times and each triple is orthogonally Walsh spread to four complex symbols. This orthogonal sequence carrying the HARQ feedback information is then robustly modulated using Binary Phase Shift Keying (BPSK) on REGs within the PDCCH. REGs used by the PHICH are shown in Figure 1.60.

1.8.12.7 Reference Signals

Reference signals are used for estimating the wireless channel leading to distortion of the received signals as described in Section 1.8. The LTE DL uses a two-dimensional spherical channel estimation procedure on frequency and time. Reference symbols are interleaved in frequency and time as can be seen in Figure 1.44 which shows the DL reference signal grid for each transmit antenna port. Furthermore, reference signals are depicted in Figure 1.60.

1.8.12.8 PSS

The PSS is a basic signal for synchronizing an LTE cell. It is primarily used for cell search and time slot synchronization. Zadoff–Chu sequences are used as PSS signals, which are sequences with an amplitude of one and varying phase shifts. Three types of PSS signals are defined, which indicate the physical c-ID group. Figure 1.62 below shows an example PSS and SSS signal as a screenshot of an IQ sample analysis dashboard. Note that the gray plane shows the IQ layer. In the third dimension the occurrence of a specific IQ combination (specific IQ vector) is depicted.

1.8.12.9 SSS

The SSS already carries the first information modulated with BPSK. After synchronizing with the SSS, the mobile has not only retrieved slot and radio frame timing, but also detected the duplex method (TDD or FDD), CP length, and the 9-bit physical layer c-ID. Figures 1.61 and 1.62 show the location of the synchronization signals within a radio frame and a subframe respectively (Figure 1.61 depicts the first subframe of a radio frame with its 14 OFDM symbols in the case of FDD and normal CP). Furthermore, note that both synchronization signals use the centered six RBs of the spectrum, but only use 62 of the 72 REs in order to gain more robustness with this spectral guard gap.

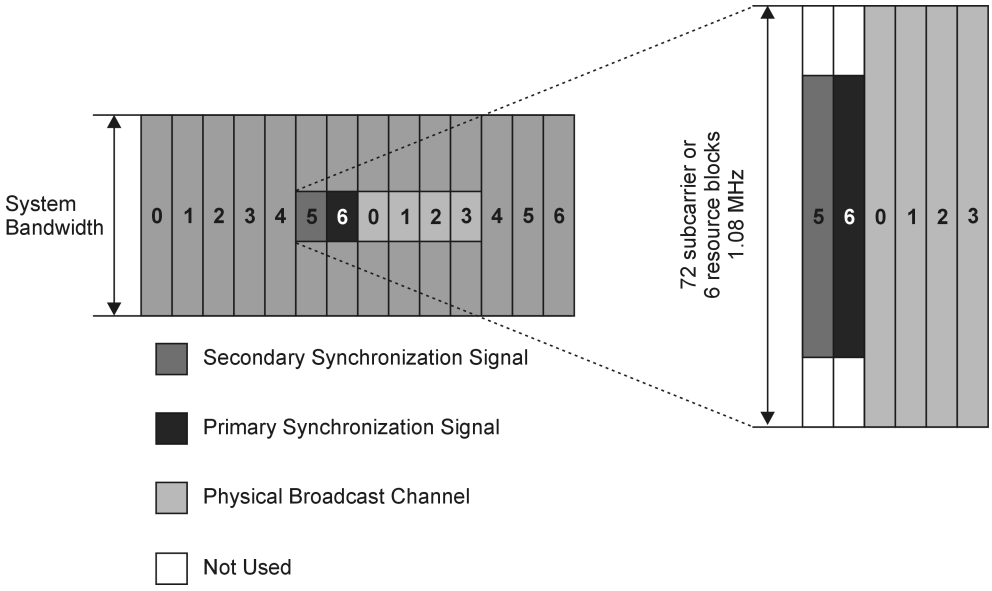


Figure 1.61 Illustration of the location of the physical broadcast channel and the primary and secondary synchronization signals within the first subframe of each radio frame. Reproduced with permission from Nomor.

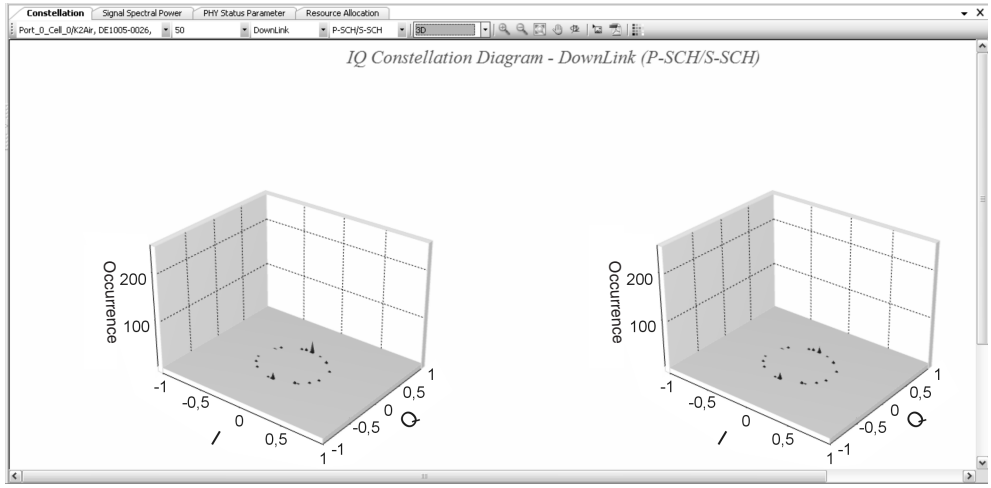


Figure 1.62 Vector IQ analysis of a primary and secondary synchronization signal on two transmit antennas.

Table 1.16 lists the applied modulation schemes for each DL channel. Physical UL channels:

- Physical Uplink Shared Channel (PUSCH).
- Physical Uplink Control Channel (PUCCH).
- Physical Random Access Channel (PRACH).

Table 1.16 Physical downlink channels and their modulation schemes

Physical downlink channel	Modulation schemes
PDSCH	QPSK, 16QAM, 64QAM
PDCCH	QPSK
PMCH	QPSK, 16QAM, 64QAM
PHICH	BPSK
PCFICH	QPSK
PBCH	QPSK

UL signals:

- Reference signal:
  - Demodulation Reference Signal (DMRS).
  - Sounding Reference Signal (SRS).

1.8.12.10 PUSCH

The PUSCH is the physical channel carrying the transport channel UL-SCH. Therefore, UL data transmission is shared channel based similar to the DL-SCH approach. The eNB assigns UL-SCH resources through UL grants transmitted via the PDCCH, see Section 1.8.9.

All UL higher layer control plane (in-band signaling) and user plane information is sent via the PUSCH using the modulation schemes of QPSK, 16QAM, or 64QAM. UL 64QAM is UE and system (signaled cell wide in an SIB) optional. PUSCH transport blocks are transmitted with a 24-bit CRC checksum.

Physical layer control information is transmitted via the PUSCH as well, in the case of parallel PUSCH and UL control information transmission.

There is no MIMO defined in the UL direction, therefore the above-mentioned transmission modes do not apply for PUSCH. The eNB has the option of selecting a transmit antenna port of the UE for the best reception.

1.8.12.11 PUCCH

UL physical layer control information (UCI) is sent via the PUCCH. The PUCCH resources are allocated at both system bandwidth edges in order to decrease interference and gain frequency diversity. UL control information is:

- **HARQ feedback**: Inner loop retransmission/reception ACK/NACK feedback.
- **Precoding Matrix Indicator (PMI)**: Used with multiple antenna transmission.
- **SR**: Used to request UL resources.
- **CQI**: DL reception quality feedback.
- **Rank Indicator (RI)**: Used with multiple antenna transmission.

Figure 1.52 depicts an example PUCCH configuration in the middle of the figure. The most important information is transmitted adjacent to the demodulation reference symbols as the channel estimation here is most accurate.

Table 1.17 Supported PUCCH formats. Reproduced with permission from © 3GPP™

PUCCH format	Modulation scheme	Number of bits per subframe, M_{bit}	Usage
1	Unmodulated	N/A	SR
1a	BPSK	1	ACK/NACK with/without SR
1b	QPSK	2	MIMO ACK/NACK with/without SR
2	QPSK	20	CQI/PMI or RI
2a	QPSK + BPSK	21	CQI/PMI or RI mux with ACK/NACK
2b	QPSK + QPSK	22	CQI/PMI or RI mux with ACK/NACK

Table 1.17 lists the defined PUCCH UCI formats with their allowed modulation schemes, number of bits per subframe, and the usage of each UL control format.

1.8.12.12 PRACH

The frequency and time location of the six consecutive RBs used for PRACH are cell-wide signaled using the SIB type 2. Zadoff–Chu sequences, forming the preamble, are transmitted after a CP as random access inquiry. Figure 1.63 shows the random access preamble format. PRACH transmissions are not UL synchronized as no UL synchronization is established yet. There are 64 preambles used within one cell, which are generated from a RACH preamble root sequence indicated in SIB type 1.

There are five random access formats defined, specifying different CP and preamble length. Four formats are used with frame type 1 which is used for FDD and the fifth format is used with frame type 2 for TDD. Diverse formats are used for different cell sizes, load, and interference conditions.

Table 1.18 lists the physical UL channels and maps the modulation schemes which are allowed for use.

1.8.12.13 DMRS

The Demodulation Reference Signals (DMRS) are defined symbols for UL channel estimation of data transmitted on the PUSCH and PUCCH. The DMRSs are located in the middle of each slot, thus on the fourth OFDM symbol. UL reference signals do not carry any information.

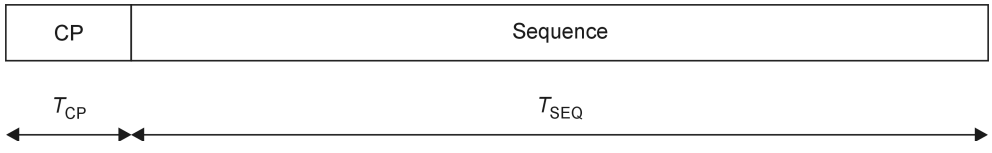


Figure 1.63 Random access preamble format (TS36.211). Reproduced with permission from © 3GPP™.

Table 1.18 Physical uplink channels with their modulation schemes

Physical uplink channel	Modulation schemes
PUSCH	QPSK, 16QAM, 64QAM
PUCCH	QPSK
PRACH	Zadoff–Chu sequences

1.8.12.14 SRS

The Sounding Reference Signal (SRS) is a signal transmitted upon request by the eNB. It is used for UE-specific UL channel quality also on frequencies which were not used for transmission previously. The eNB requests the UEs to transmit an SRS symbol on parts of the bandwidth or on the complete system bandwidth. SRS transmission takes place always on the last OFDM symbol of the subframe, if it is requested.

1.8.13 Transport Channels in LTE

The physical layer provides a transport service for MAC PDUs. This service is accessed by transport channels. Most transport channels are directly mapped to physical channels as described in Section 1.8.14. Thus, in other words, transport channels are the gateway to physical channels and a selection for MAC PDUs where they are to be transmitted.

The following DL transport channel types are defined:

- **Broadcast Channel (BCH)**:
  - Uses a static transport format and has the requirement that all UEs within the cell have to receive its information error-free. The reception of the BCH is mandatory for accessing any service of a cell.
- **DL-SCH**:
  - Carries all semi-static broadcast information (SIB) and all UE-specific traffic channels.
  - DL-SCH is secured with HARQ algorithms.
  - Efficiency is realized with AMC link adaptation.
  - Various TMs are defined to meet different environment scenarios to increase efficiency in respect of current conditions.
  - DRX is available in order to increase handset operating time.
  - Makes use of spatial algorithms like beamforming or MIMO.
- **Paging Channel (PCH)**:
  - Needs to be received in complete cell coverage area.
  - Supports DRX in order to increase battery operating cycle.
  - Dynamically allocated via own physical identifier (P-RNTI).
- **Multicast Channel (MCH)**:
  - Broadcast to entire cell coverage area.
  - MBMS transmission with use of multiple cells.

A designated DL control channel is not defined as the PDCCH is used for physical channel control only. All the higher layer control plane is transmitted via the DL-SCH.

Defined UL transport channel types are shown in the following items:

- **UL-SCH**:
  - UL-SCH is secured with HARQ algorithms.
  - Fully dynamic and semi-static resource allocation schemes.
  - Can make use of multi-user MIMO (UL “virtual” MIMO).
  - Uses dynamic link adaptation like AMC.
- **RACH**:
  - Accessible without UL synchronization.
  - Collision-based and collision-free operating modes.
  - Various modes depending on cell size and interference.

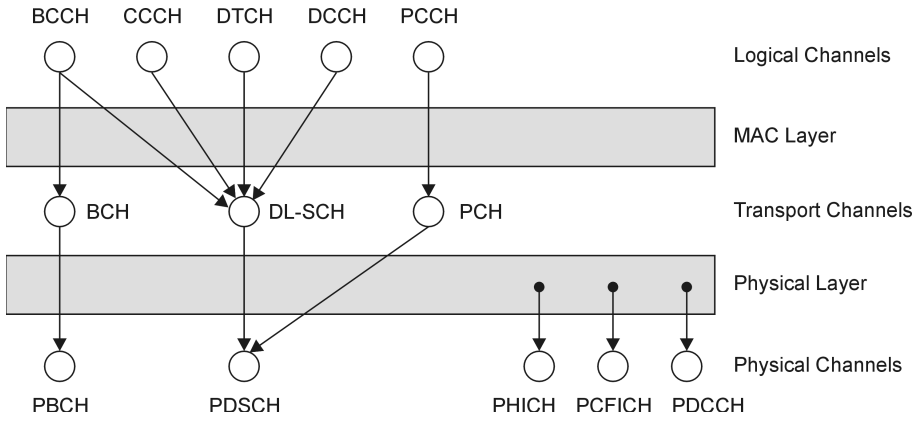


Figure 1.64 Downlink channel mapping and multiplexing from logical channels via transport channels to physical channels.

As in the DL direction, no UL control transport channel is defined as all the higher layer control plane is transmitted on the UL-SCH. The PUCCH is a control channel used by the physical layer only.

1.8.14 Channel Mapping and Multiplexing

Besides physical and transport channels, LTE also defines logical channels. Logical channels are multiplexed to transport channels within the MAC layer. Logical channels map different content connections to transport channels, like CCCHs to multiple UEs or DCCHs to a specific UE or dedicated transport channels carrying higher layer application data.

Logical channels are addressed with a logical channel ID. The logical ID is a field within the MAC header PDU. Logical channels are multiplexed by using logical channel IDs to transport channels specifying where the information should be transmitted. Finally, transport channels are transferred with physical channels as a service provided by the physical channel.

Figures 1.64 and 1.65 show the above-described channel architecture from the basic physical channels via transport channels to logical channels bearing higher layer messages for DL and UL respectively.

Two basic sets of logical channels are defined:

- **Control channels**: CCCH and DCCHs.
- **Traffic channels**: CCCH and DTCHs.

The nature of common channels is such that no specific UE is addressed, but the information is either general for all cell-wide subscribers or a message from a UE which has not yet established a dedicated control/traffic channel. A typical example of a CCCH is the broadcast of SIBs.

Traffic channels carry user plane protocols like the Packet Data Convergence Protocol (PDCP) and application IP packets, while control channels carry control plane protocols as RRC and NAS.

- **DL logical channels**:
  - Broadcast Control Channel (BCCH).
  - Paging Control Channel (PCCH).

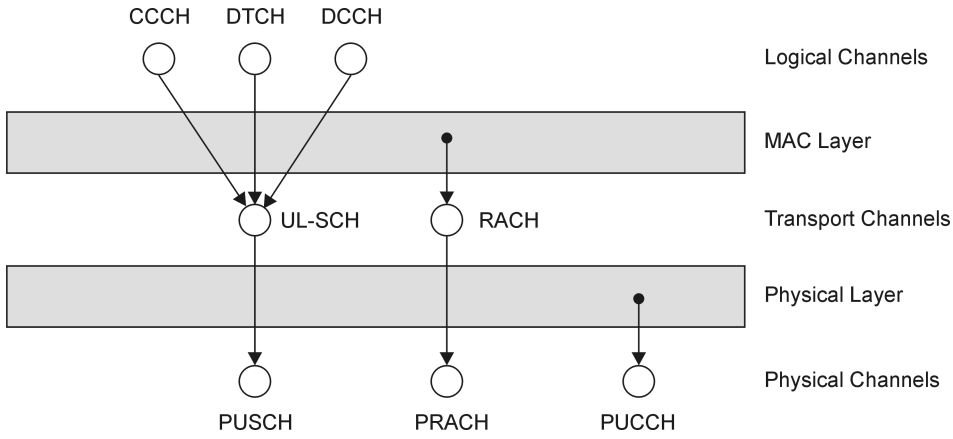


Figure 1.65 Uplink channel mapping and multiplexing from logical channels via transport channels to physical channels.

- Common Control Channel (CCCH).
- Dedicated Control Channel (DCCH).
- Dedicated Traffic Channel (DTCH).

• **UL logical channels**:

- Common Control Channel (CCCH).
- Dedicated Control Channel (DCCH).
- Dedicated Traffic Channel (DTCH).

Logical Channel Identifiers (LCIDs) are depicted in Section 1.10.4.

1.8.15 Initial UE Radio Access

Cell search is a procedure for synchronizing time and frequency to a base station sector. Additionally, cell search and synchronization include deriving basic information of the target cell.

LTE defines a hierarchical cell search as it is deployed with WCDMA UMTS. PSS and SSS provide radio frame and slot synchronization, as well as information like the duplex mode TDD or FDD and the physical layer group and c-ID.

UEs synchronizing to a new LTE cell start searching for a PSS which is a Zadoff–Chu sequence. Three sequences are defined indicating the physical cell group ID. Three physical layer c-ID groups with 168 physical layer c-IDs each are defined. After successfully detecting the PSS with its physical layer c-ID group and slot timing, the SSS is decoded which is broadcasted one OFDM symbol prior to the PSS. Now the UE retrieved DL slot, radio frame timing and frequency synchronization. With decoding successfully PSS and SSS, it obtained as well the complete 9-bit physical layer c-ID together with the radio frame type (either type 1 for FDD or type 2 for TDD) and the CP length.

Figure 1.66 illustrates the initial steps of cell synchronization and access. After synchronization, the UE is ready to detect and decode the PBCH in order to derive the system bandwidth, PHICH configuration, and the current System Frame Number (SFN). Other common system information now needs to be retrieved from the DL-SCH. SIBs are scheduled on regular shared channel resources by

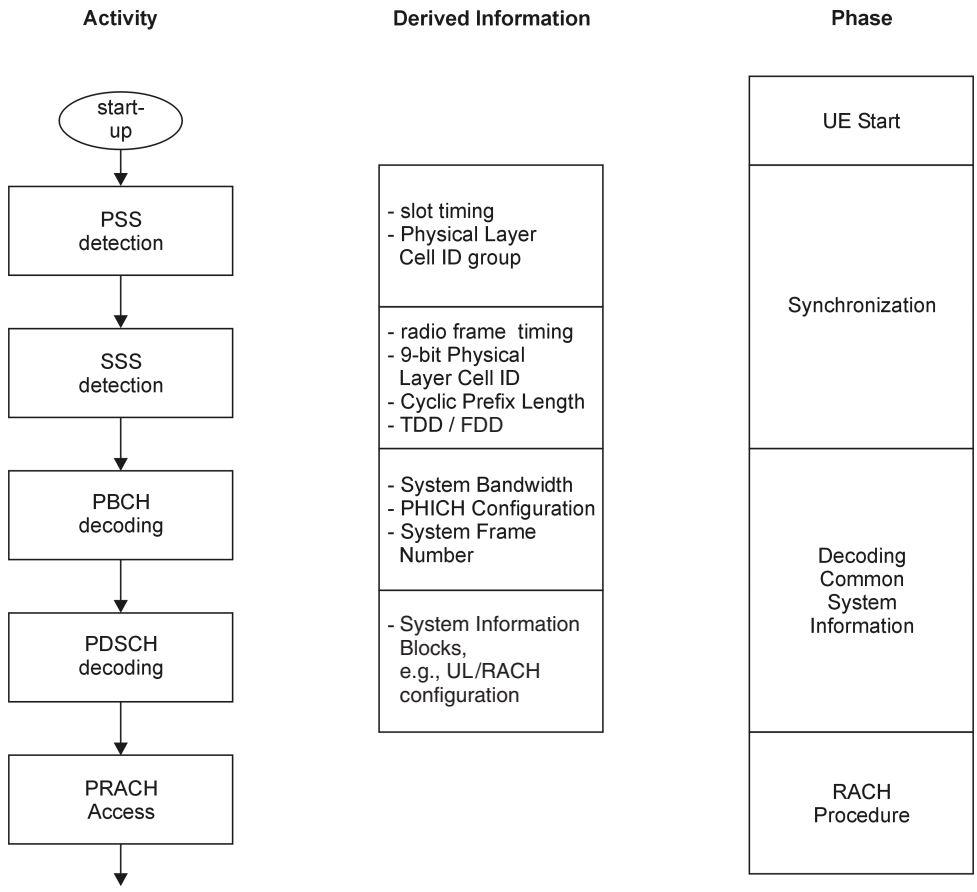


Figure 1.66 Initial cell access with level of retrieved information.

using a special C-RNTI = 0xFFFF. SIBs provide general system configuration information like UL configuration and random access configuration.

With the procedure described above, the UE is ready to access the random access procedure outlined in the next section.

1.8.16 UE Random Access

A UE random access is performed not just with the UE initial access to the network, but for various other reasons. Especially in LTE, the random access procedure is a central UE procedure as the physical transport channel architecture is shared channel based and only two RRC states are defined: RRC_CONNECTED and RRC_IDLE. FDD and TDD define a common random access procedure. The PRACH is designed in such a way that the same routine and format is used for all cell sizes (long propagation delay and long channel echo spread) and just some configuration parameters can be changed in order to cope with various cell conditions, as described in Section 1.8.12.

The following items outline the events in which a random access procedure should be made:

- At UE initial access.
- For RRC connection re-establishment, for example, when radio link failures occur.
- When handovers are triggered, usually a contention-free RACH procedure is configured.
- In case of no UL synchronization and arrival of DL data.
- In case of no UL synchronization and UL data is to be transmitted.
- In case UL data is to be transmitted but no PUCCH resources are available to indicate a SR.

Two random access procedures are defined to distinguish an eNB-initiated RACH procedure against a completely independent RACH access:

- **Non-contention based**: The eNB assignment of used RACH resources in cases of handover and DL data arrival. Collisions should not occur.
- **Contention based**: In previously fully unknown RACH resources because of random selection by UEs accessing a cell, for example, initial access or radio link failure. Collisions might occur.

The nature of the PRACH is described in Section 1.8.12. The contention-based RACH procedure is described in the following.

Figure 1.67 illustrates the contention-based RACH procedure with its four messages. A UE selects a random access preamble and transmits it in the time and frequency resources of the PRACH with initial RACH power settings derived from SIBs. This is depicted in Figure 1.67 as message 1.

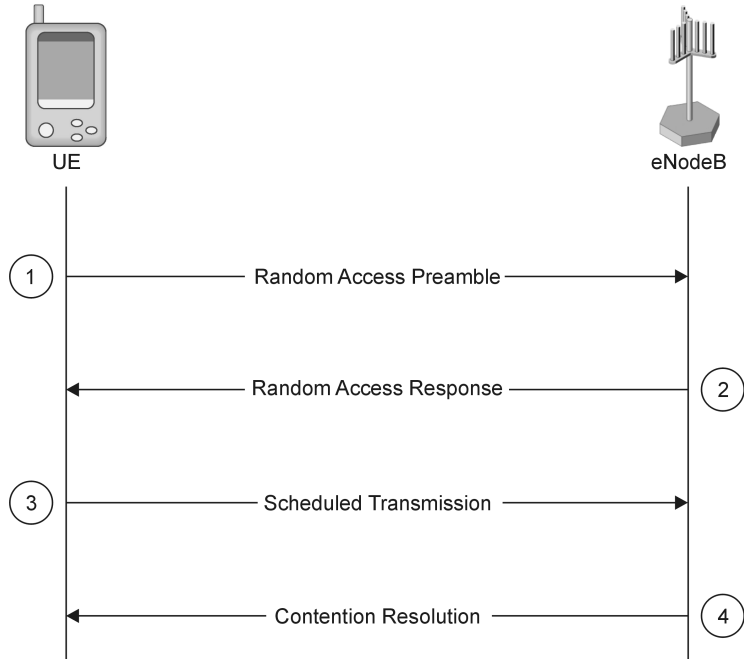


Figure 1.67 Contention-based random access procedure (TS36.300). Reproduced with permission from © 3GPP™.

Now the UE starts to monitor the PDCCH for a DL response from the eNB. This RAR is transmitted in the time-wise RAR window (message 2). Within this window, the UE originating the RACH preamble listens to the scheduled RAR with a special identifier called a Random Access Radio Network Temporary Identifier (RA-RNTI) matching the RACH time slot where its RACH preamble was transmitted. The RA-RNTI is calculated by the following equation:

$$\text{RA-RNTI} = 1 + \text{t\_id} + 10*\text{f\_id}$$

where t_id addresses the first subframe of the used PRACH, resulting in a possible range between 0 and 9, and f_id is the ascending frequency index within this subframe with a range between 0 and 5. Thus, the RA-RNTI has a range

$$1 \leqslant \text{RA-RNTI} \leqslant 60$$

in decimal or, in 16-bit hexadecimal,

$$0\text{x}0001 \leqslant \text{RA-RNTI} \leqslant 0\text{x}003\text{c}$$

All received preambles within one PRACH are answered by one MAC PDU containing multiple RAR messages addressing random access identifiers matching the preamble index used by a specific UE. Each preamble indicates a single UE random access attempt which is addressed and answered by one MAC RAR as depicted in Figures 1.68 and 1.69.

A new preamble with additional power is transmitted if there is no RAR message received within the RAR window by a UE which has sent a preamble. This random access power ramping procedure

B7	LTE-RLC/MAC (MAC-RAR (DL))	3GPP LTE-RLC/MAC Rel.8 (MAC TS 36.321
B7	1 MAC Random Access Response	
01101110	1.1 MAC RAR Header Part	
01101110	1.1.1 MAC Random Access ID Subheader	
0-------	Extension field	Last MAC PDU subheader
-1------	Type Field	Random Access Identity
--101110	Random Access Identity	46
B6	1.2 MAC RAR Payload Part	
B6	1.2.1 MAC Random Access Response	
0-------	Reserved	0
b11*	Timing Advance Value	2
b20*	UpLink Grant Resources	'00000001010010001100'B
B2	Temporary C-RNTI Value	'a277'H

Figure 1.68 Example RAR message.

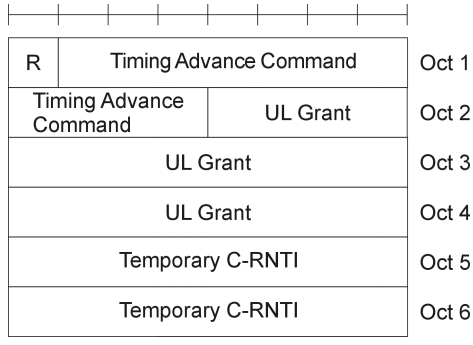


Figure 1.69 A 6-byte MAC RAR (TS36.321). Reproduced with permission from © 3GPP™.

is repeated until a RAR message for its preamble is received or the maximum allowed transmit power is reached.

An initial timing advance command is calculated by the eNB in order to synchronize all UL traffic to the orthogonal UL slot structure. A first physical layer address, the temp C-RNTI, is assigned to the UE with the RAR message.

Furthermore, the RAR message carries a 20-bit UL grant field containing the following information:

- Hopping flag – 1 bit.
- Fixed size UL resource block assignment for the first scheduled UL transmission in the PUSCH – 10 bits.
- Truncated MCS – 4 bits.
- TPC command for above scheduled UL transmission – 3 bits.
- UL delay – 1 bit.
- CQI request – 1 bit.

Other than TPC commands within an established connection (1-bit or 2-bit TPC commands), the TPC command within the MAC RAR message consists of 3 bits addressing the power adjustment range, as in Table 1.19.

The first scheduled UL transmission on the PUSCH (RACH contention-based procedure message 3) takes place after decoding the correct RAR message. This RACH procedure message number 3 is, for example, the rrcConnectionRequest in case of a UE initial access and the rrcReestabilishment after, for example, a radio link failure or the rrcConfigurationComplete in case of a Hand Over (HO). It is mandatory to use the RACH contention-based procedure in both cases because the eNB cannot assign RACH resources previously in order to prevent RACH collisions.

The contention resolution message number 4 mirrors the RACH procedure message number 3 which includes at least a NAS identifier. This message is used to detect collusions as each UE compares its transmitted message number 2 (message 3 of the RACH procedure as depicted in Figure 1.67) with the received contention resolution payload field.

A non-contention-based RACH procedure is defined as illustrated in Figure 1.70. This procedure is used in cases of handover and DL data arrival in the UL non-synchronized state.

Message number 0 assigns a random access preamble to the UE which is not broadcast for the contention-based RACH procedure. This is done on the source eNB triggered by a handover command via the X2 interface from the target eNB in the case of handover. It is signaled via the PDCCH on DL data arrival.

The assigned random access preamble is used within the PRACH resources of the target eNB or on PRACH in case of DL data arrival.

Table 1.19 TPC command δ_{msg2} in RAR for scheduled PUSCH UL grant. Reproduced with permission from © 3GPP™

TPC command	Value (in dB)
0	−6
1	−4
2	−2
3	0
4	2
5	4
6	6
7	8

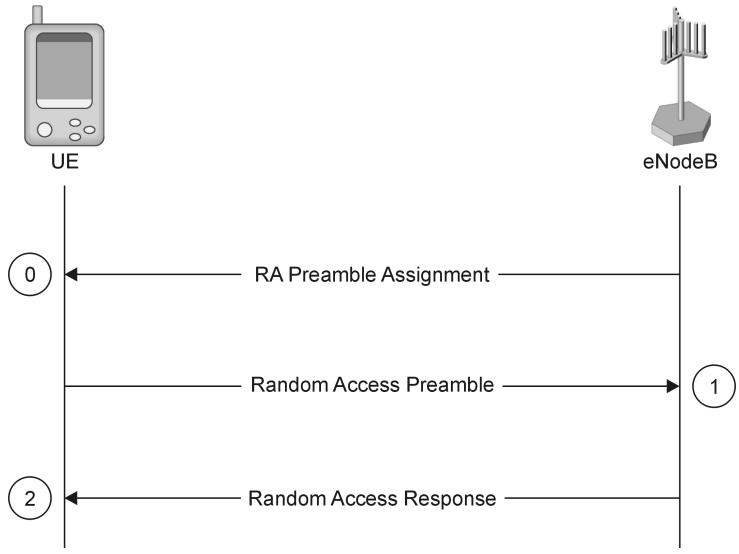


Figure 1.70 Non-contention-based random access procedure. Reproduced with permission from © 3GPP™.

Message number 2 is the RAR message similar to the contention-based procedure but a Temp C-RNTI assignment is not mandatory as the UE might already have an RNTI assigned.

Regular UL and DL transmission can take place after the random access procedure as all mandatory parameters are known by both sides and UL synchronization is established.

1.9 LTE Network Protocol Architecture

1.9.1 Uu – Control/User Plane

The protocol stack used on radio interface Uu is shown in Figure 1.71. The physical layer in this stack is represented by OFDM in the DL and SC-FDMA in the UL. Then we see the MAC protocol that is

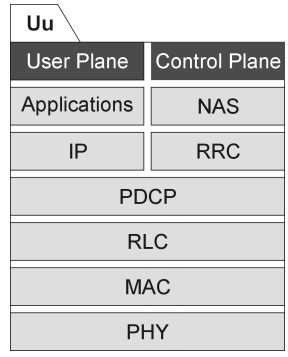


Figure 1.71 Protocol stack LTE Uu interface.

responsible for mapping the transport channels onto the physical channels, but also for such important tasks as packet scheduling and timing advance control. RLC provides reliable transport services and can be used to segment/reassemble large frames. The main purpose of PDCP is the compression of larger IP headers as well as ciphering of user plane data and integrity protection of both user plane and control plane data.

On top of PDCP the stack is split into the user plane and control plane parts. On the control plane side we see RRC protocol, that is, the expression for the communication between the UE and eNB. RRC provides all the necessary functions to set up, maintain, and release a radio connection for a particular subscriber. Details of these functions are described in Section 1.10.7.

RRC also serves as a transport protocol for NAS signaling messages. NAS is the expression for the communication between the UE and MME in which MME represents the core network.

On the user plane side we see IP as the transport layer for end-to-end applications. On the Uu stack the IP is always end-to-end IP, which means that all these IP packets are transparently routed, often tunneled through the mobile network. The user plane IP frames we see on Uu are the same IP frames that can be monitored at SGi reference points before or behind the PDN-GW.

The IP version can be Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6). In the case of VPN (Virtual Private Network) traffic, IPsec will be used.

The applications on top of IP in the user plane stack are all protocols of the TCP/IP suite, such as the File Transfer Protocol (FTP), HTTP (web-browsing), and POP3/SMTP (for e-mail), but also Real-Time Transport Protocol (RTP) and SIP for real-time services like VoIP.

1.9.2 S1 – Control/User Plane

On the S1 reference point the physical layer L1 will in most cases be realized by Gigabit Ethernet cables. L2 in this case will be Ethernet. On top of Ethernet we find IP, but used as a transport protocol between two network nodes: eNB and MME. This lower layer IP does not represent the user plane frames.

Instead, the user plane IP frames (higher layer IP) are carried by the GTP Tunneling Packet Data Unit (T-PDU). The GTP is responsible for the transport of payload frames through the IP tunnels on S1-U. The transport layer for GTP-U is the User Datagram Protocol (UDP). As IP this protocol may be found twice in the user plane stack: lower UDP for transport between the eNB and MME and higher UDP (not shown in Figure 1.72) that is transparently routed through the mobile network as the

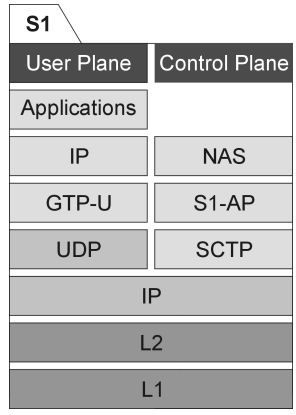


Figure 1.72 Protocol stack S1 control/user plane.

transport protocol for real-time application data. The higher layer IP on top of GTP-U as well as all application data on top of this higher layer IP are identical with the user plane information described in the previous section.

On the control plane side, the Streaming Control Transport Protocol (SCTP) provides reliable transport functionality for the very important signaling messages. S1AP is the communication expression between MME and S-GW while NAS – as already explained in the previous section – is used for communication between the UE and MME.

1.9.3 X2 – User/Control Plane

On the X2 interface the user plane protocol stack is identical to that of the S1 reference point. However, as shown in Figure 1.73, on the control plane there is a different protocol: X2 Application Part (X2-AP).

The main purpose of X2-AP is to provide inter-eNB handover functionality. It also is used to exchange traffic-related and radio quality measurement reports between different eNBs.

1.9.4 S6a – Control Plane

There is no user plane at the S6a reference point due to the fact that we find here the connection between the MME and HSS, which is a plain signaling communication.

L1, L2, IP, and SCTP shown in Figure 1.74 provide the same functionality as explained in the section on the S1 protocol stack.

The new player in the S6a stack is the DIAMETER protocol. In the EPC network DIAMETER has taken over the role of the Mobile Application Part (MAP). It is used to update the HSS about the current location of the subscriber and to provide crucial subscriber attributes stored in HSS databases to the MME so that network access can be granted and the subscriber's traffic can be routed according to these parameters. DIAMETER is also involved in the security functions of the network: subscriber authentication, integrity protection, and ciphering.

The protocol stack on S6a is identical to the protocol stack of the S13 reference point between the MME and EIR – in case an EIR exists in the network.

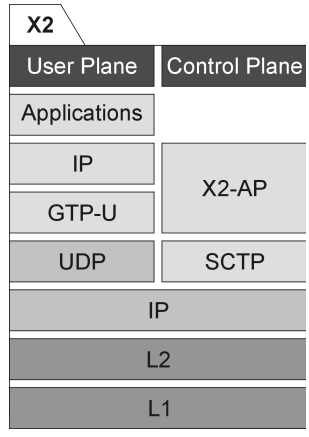


Figure 1.73 Protocol stack X2 control/user plane.

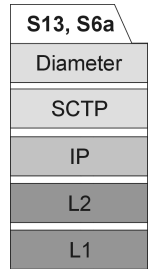


Figure 1.74 Protocol stack S6a.

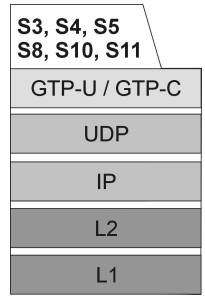


Figure 1.75 Protocol stack S3S4/S5/S8/S10/S11.

1.9.5 S3/S4/S5/S8/S10/S11 – Control Plane/User Plane

At the S3, S4, S5, S8, S10, and S11 reference points we find the same protocol stack as shown in Figure 1.75. The reason is that all these interfaces are used to tunnel IP payload transparently from one network node to the other. The tunnel management is provided by GTP-C while the IP payload is transported using GTP-U T-PDUs. Indeed, the user plane protocol stack is the same as on the S1 reference point.

Simplifying the functionality of GTP-C, it can be said that this protocol is used to create, modify, and delete user plane tunnels. It also supports mobility of subscribers between core network nodes.

1.10 Protocol Functions, Encoding, Basic Messages, and Information Elements

1.10.1 Ethernet

Ethernet is the typical transport layer protocol in IP networks. It is designed to transmit packets from a sender to a receiver, both identified on behalf of an address information element.

According to this limited functionality, Ethernet has a very small header. The header field (Figure 1.76) contains only the information elements:

- Destination address.
- Source address.
- Ethernet type.

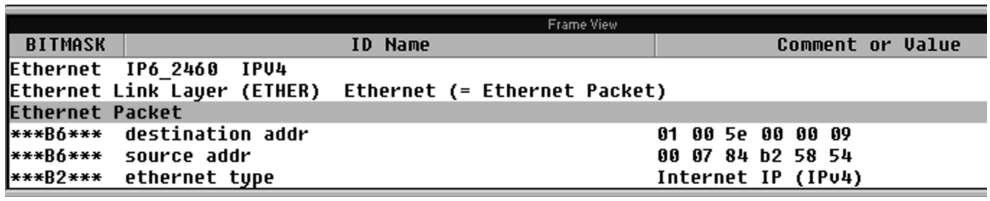


Figure 1.76 Ethernet header example.

Ethernet type is similar to a SAPI (Service Access Point Identifier). It contains information about which higher layer protocol information is transported by Ethernet frames.

The Ethernet addresses, often called MAC addresses (but with nothing in common with RLC/MAC!), consist of 6 bytes. These MAC addresses are fixed hardware addresses and, due to a defined numbering scheme, each address is unique worldwide.

If IP data is to be transmitted using Ethernet the hardware MAC address of the receiver of IP packets is unknown when the connection starts. Only the target IP address is known. However, since Ethernet is the lowest layer of the connection there must be a source and a destination MAC address included in each header. In other words, for each sender IP address there is an appropriate sender hardware address, and for each destination IP address there must be an appropriate target hardware address.

The target hardware address that is related to the target IP address is requested by the Address Resolution Protocol (ARP). Its sister protocol, the Reverse Address Resolution Protocol (RARP), can be used to find the target IP address (or, in terms of ARP/RARP, the target protocol address) to a known MAC address.

The address resolution procedure consists of two steps:

1. ARP request (req) message with Target Hardware Address = "0" is sent to *all(!)* IP clients in the network.
2. The client that has the target protocol address as set in the ARP req message sends ARP Replay (rpl). The sender hardware address in ARP rpl is the Ethernet MAC address related to the destination IP address that the sender of the ARP req is looking for. An example of the Ethernet address resolution procedure is shown in Figure 1.77.

1.10.2 Internet Protocol (IPv4/IPv6)

The IP frame is called the datagram and there exist two main versions of the IP: IPv4 and IPv6.

1.10.2.1 IPv4

The IP header has a minimum size of 20 bytes (if no options are used) and a maximum size of 64 bytes (including options and padding bits). Due to a set of different options that can be appended to the IPv4 header, these headers can become very large.

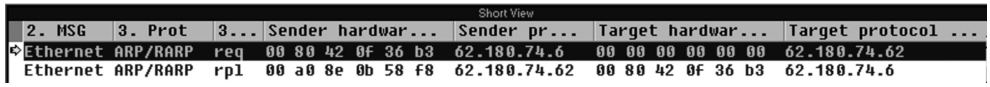


Figure 1.77 Ethernet address resolution.

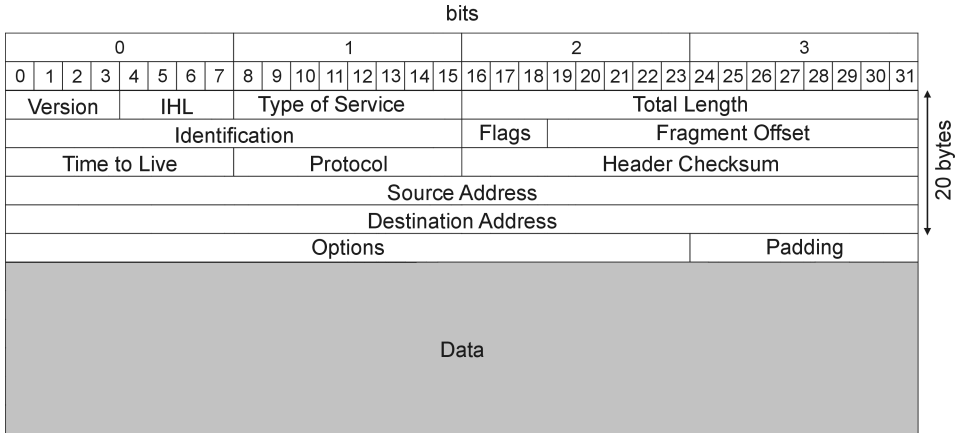


Figure 1.78 IP datagram structure.

The included information elements shown in Figure 1.78 are:

- **Version**: IP protocol version, here IPv4.
- **Internet header length** (IHL length): The length of the header.
- **Type of Service**: The QoS parameters for IP.
- **Total Length**: The length of the IP frame including header and payload field.
- **Identification, Fragment Offset**: Both used in case of fragmentation/reassembly.
- **Time to Live**: A hop counter to prevent circular routing.
- **Protocol**: Indicates the higher layer protocol that uses IP as the transport layer; typical examples are ICMP, TCP, UDP.
- **Source Address**: IP address of the sender of the datagram.
- **Destination Address**: IP address of the receiver of the datagram.
- **Options**: For example, the timestamp of each router that the IP packet passed.
- **Padding**: Fill bits to align the header to a multiple of 32 bits.

Since the maximum packet size of an IP datagram can vary from one local network to the next, the IP is equipped with fragmentation/reassembly functionality that allows the transmission of larger frames in series of smaller portions. Figure 1.79 shows an example where a frame with 1600 bytes of data is fragmented into two smaller frames with 1480 and 120 bytes of data each. Fragmented frames do all have the same frame ID (in the example: 1234). As long as more fragments are following the first one, the fragmentation flag MF is set to "1." The last frame in a series of fragments has fragmentation flag MF = "0," but a fragmentation offset that is required for proper reassembly on the receiver side.

IP fragmentation (Figure 1.79) may be found in the user plane data streams, but should be avoided on interfaces that carry 3GPP signaling.

IPv4 addresses are typically written in the so-called dotted decimal notation, for example, 195.24.1.2. There are 32 bits (= 4 bytes) reserved for the address fields in the IP datagram. Each number in the dotted decimal format represents the decimal value of a single byte. The dot "." is used as the separator between the different bytes of the IP address. Figure 1.80 shows a sample address in binary, hexadecimal, and decimal dotted notation format.

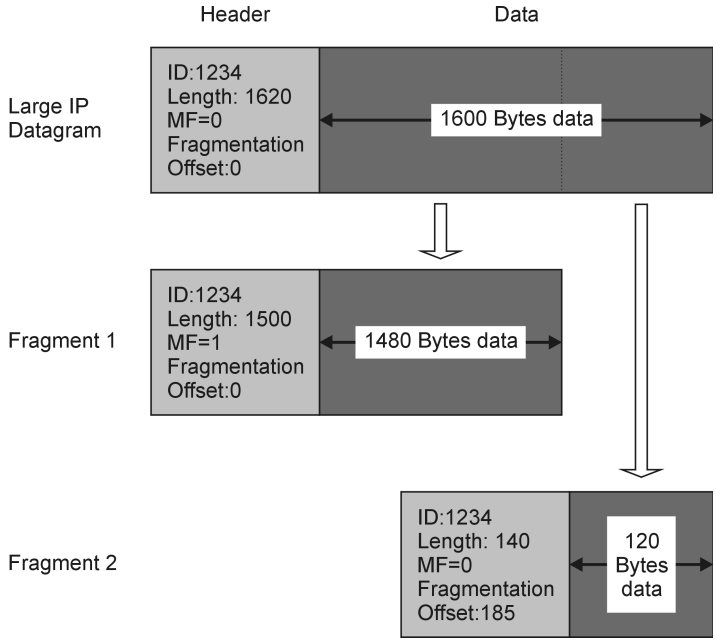


Figure 1.79 IP fragmentation.

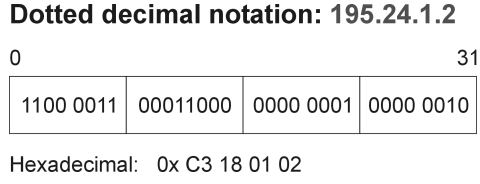


Figure 1.80 Example of IPv4 address format.

1.10.2.2 IPv6

The most important improvements that come with IPv6 are:

- A larger number of possible address values become available. In IPv4 the number of addresses is limited to 32 bits, which means in turn that 2^{32} (≈ 4.3 billion $= 4.3 \times 10^9$) possible values can be addressed. IPv6 provides space for 2^{128} ($= 3.4 \times 10^{38}$) possible address values. This is an improvement by a factor of 2^{96} and reached by a restructuring of the IP header. In the IPv6 header shown in Figure 1.81, 128 bits (16 bytes) is reserved for source and destination addresses. The larger address ranges available for IPv6 will also allow more direct end-to-end packet routing and, hence, less address translation in network nodes is required and the packet routing in the overall network is expected to be faster and more efficient.
- The automatic configuration of dynamically assigned IP addresses is improved and in turn legacy procedures like DHCP (Dynamic Host Configuration Protocol) become unnecessary.

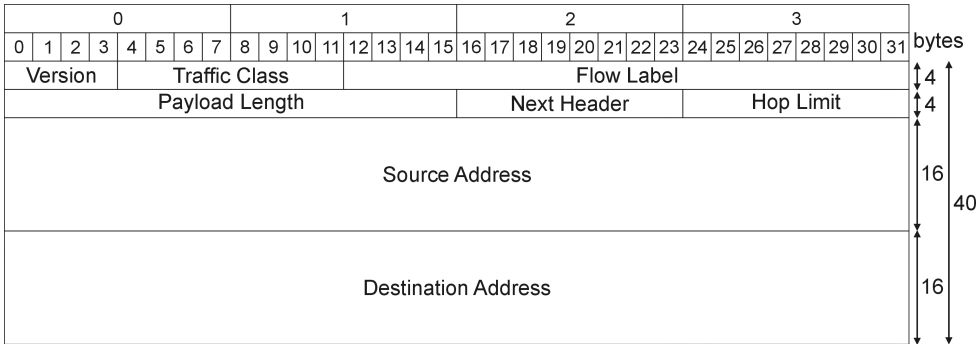


Figure 1.81 IPv6 header format.

- IPv6 supports Mobile IP, simplifies renumbering (change of dynamically assigned IP addresses), and allows multihoming of subscribers. The purpose of multihoming is to increase the reliability of Internet connections by using two different Internet service providers simultaneously. If the access to one of the providers is interrupted a redirection of packets via the second connection is possible. Mobile IP means that the subscriber always gets the same IP address assigned, no matter if working at home or traveling around.
- IPsec is integrated into IPv6 to achieve a higher security of IP data transmission, while back in IPv4 no security functions were provided at all.
- All in all, the basic header of IPv6 has a simpler structure compared to the header of IPv4. Although the overall header size is larger than in IPv4 (40 bytes, most of them occupied by the longer IP addresses), there are less basic header fields.
- For the version, the decimal number 6 is encoded as binary bit sequence "0110."
- The IPv6 traffic class indicates the packet priority and should not be mistaken for the traffic class QoS element introduced in 3GPP standards that classifies the throughput sensitivity and delay sensitivity of application services. IPv6 traffic class priority values subdivide into two ranges: traffic, where the source provides congestion control, and non-congestion control traffic.
- The flow label is used for QoS management and encoded in 20 bits. Packets having the same flow label value will be treated with the same priority and reliability. This is important for the routing of packets that contain real-time service data.
- The payload length indicates the size of the payload in octets and is encoded in 16 bits. When cleared to zero, the option is a "Jumbo Payload" (hop by hop). The size of the basic header is not counted by the payload length, but the optional header extensions are included. So payload length + 40 bytes (of basic header) = total length of the IPv6 packet.
- The next header information element specifies the next upper layer protocol of the transported payload such as UDP and TCP. The values are compatible with those specified for the IPv4 protocol field (8 bits). The next header information can also point to optional extension headers. In this case the upper layer payload protocol is not indicated by this field.
- The hop limit field (8 bits) indicates the maximum number of routers that are allowed to be involved in routing an IPv6 packet. It replaces the time to live field of IPv4. If the hop limit reaches the value "zero" the packet will be discarded by the router.
- Source and destination addresses, 128 bits each, represent the sender and receiver of the IPv6 datagram.

IPv6 addresses are normally written as eight groups of 16 bits, where each group is separated by a colon (:). For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 is a valid IPv6 address.

To shorten the writing and presentation of addresses, several simplifications to the notation are permitted. Any leading zeros in a group may be omitted; thus, the given example becomes: 2001:db8:85a3:0:0:8a2e:370:7334.

Also, one or any number of consecutive groups of value 0 may be replaced with two colons (::): 2001:db8:85a3::8a2e:370:7334.

It is possible to use IPv6 addresses in the URL notation format. In this case the IPv6 address information is enclosed in square brackets:

http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]/.

The brackets prevent that part of the IPv6 address being misinterpreted as port number information. A URL including IPv6 address and port number looks like this:

http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:8080/.

1.10.3 Stream Control Transmission Protocol (SCTP)

Originally the SCTP was defined as a transport protocol for SS7 messages to be transmitted over IP networks. As TCP and UDP it is seen as a layer 4 transport protocol in the ISO OSI model.

The SCTP frames are called chunks. All chunks are associated to a connection that guarantees in-order delivery. However, within the same chunk there might be data blocks of different connections transmitted simultaneously. In addition, it is also possible to send urgent packets "out of order" with a higher priority.

SCTP also supports multihoming scenarios where one host owns multiple valid IP addresses.

Besides the data streams, SCTP frequently sends heartbeat messages to test the state of connection.

How SCTP works will be demonstrated by means of an example. Figure 1.82 shows the message flow required to transport the NAS signaling message Attach Request from the eNB to MME across the S1 interface.

After setting up a RRC connection on the Uu interface between the UE and the eNB, the UE sends the attach request message. When the appropriate RRC transport container is received by the eNB, the establishment of a dedicated SCTP stream on the S1 interface as shown in Figure 1.82 is triggered.

The establishment of the SCTP stream starts with a SCTP initiation message. It will always be sent by the eNB in the case of the attach procedure, because the RRC connection is established earlier and the request to transport the NAS message triggers the request to have a S1 connection. The SCTP initiation message contains the IP addresses of both the eNB and MME. The individual subscriber for which this connection is established is represented by a unique pair of SCTP source port and destination port numbers.

The SCTP initiation needs to be acknowledged by the peer SCTP entity in the MME. In the next step a SCTP cookie echo message is sent and acknowledged by Cookie Echo ACK. In the protocol world, this is called a heartbeat procedure. Such a procedure periodically checks the availability and function of the active connection. Similar functions with other message names are found, for example, in SS7 SCCP Inactivity Test or GTP Echo Request/Response.

On SCTP higher layer messages are transported using SCTP datagram (SCTP DTGR) packets. Each SCTP DTGR contains a Transaction Sequence Number (TSN) in addition to source and destination address information. This TSN will later be used by the peer entity to acknowledge the successful reception of the DTGR by sending an SCTP selective ACK message on S1 that confirms error-free reception of the SCTP DTGR that carried the attach request message. Further S1AP and NAS messages of this connection will be transported in the same way and the Cookie Echo/Cookie Echo ACKs will be sent periodically as long as the connection remains active.

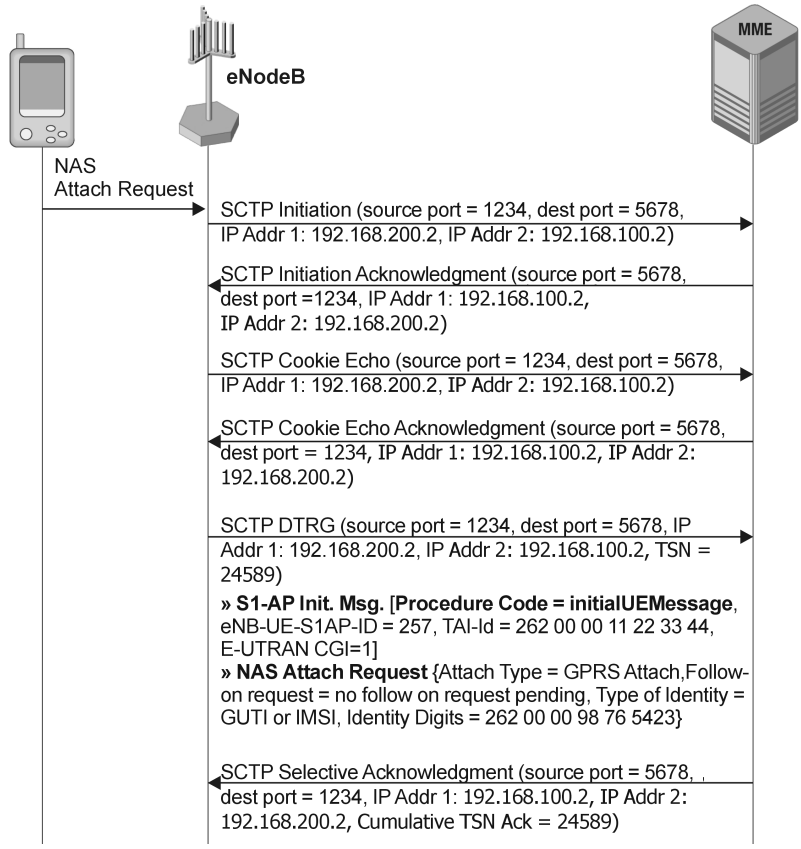


Figure 1.82 SCTP example.

If the S1 signaling transport layer SCTP has problems in offering proper functionality, there will be no signaling transport on S1 if the problems are located in the eNB SCTP entity. If the MME suffers from congestion or protocol errors on the SCTP level as shown in Figure 1.83, the expected selective ACK messages will be missing (maybe not sent at all, maybe sent with a TSN out of the expected range). This malfunction may be detected by a NACK Cookie Echo and as a result the connection will be terminated. Or the attach accept message expected to be received by the UE will be missed. The missing attach accept message will be recognized by the UE where a timer is guarding the NAS procedures. After the guard timer expires on the UE side the attach request message will be repeatedly sent up to n times (the counter value of n is configurable and typically signaled on the broadcast channel SIBs; the default value recommended by 3GPP is $n = 5$). If neither an attach request message nor an attach reject message is received by the UE the handset will go back to IDLE when the maximum number of attach request repetitions has been sent.

1.10.4 Radio Interface Layer 2 Protocols

LTE splits the layer 2 into three sublayers: MAC layer, RLC layer, and PDCP layer. Figure 1.84 illustrates the layer 2 architecture for DL and Figure 1.85 that for UL.

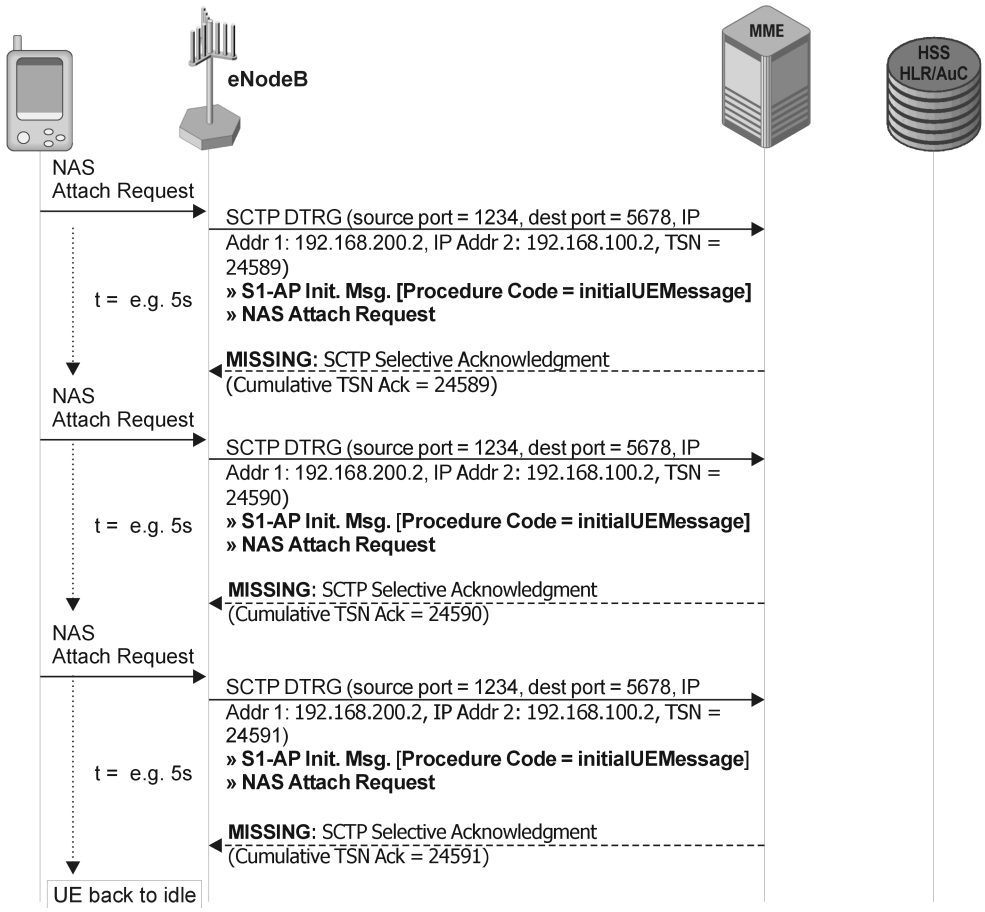


Figure 1.83 Failure in SCTP signaling transport.

The sublayers (sublayers are called layers in the following) communicate via Service Access Points (SAPs). A lower layer provides services to the adjacent layer above through SAPs. From the point of view of the lower layer, the packets providing this service are Service Data Units (SDUs). This layer once more uses services from a lower layer, again by giving its packets through SAPs to the adjacent lower layer. Those packets are called Packet Data Units (PDUs). Hence, a PDU from a higher layer is a SDU from the point of view of the lower layer providing a service to the higher layer.

SAPs are depicted as ovals between the layers in Figures 1.84 and 1.85.

Each layer with its unique functionality is introduced in the next three sections.

1.10.5 Medium Access Control (MAC) Protocol

The MAC layer provides services through SAPs to the upper layer as all other sublayers of layer 2. The layer above MAC is the RLC layer (see Section 1.10.6); the lower layer is the physical layer which provides services to the MAC. In the case of the MAC, SAPs to the RLC layer are logical

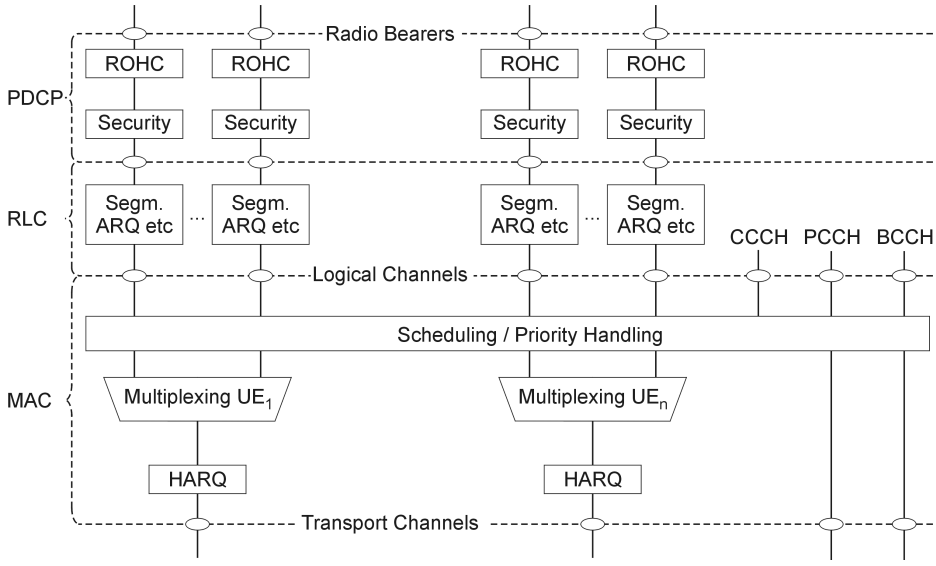


Figure 1.84 Layer 2 structure for DL (TS36.300). Reproduced with permission from © 3GPP™.

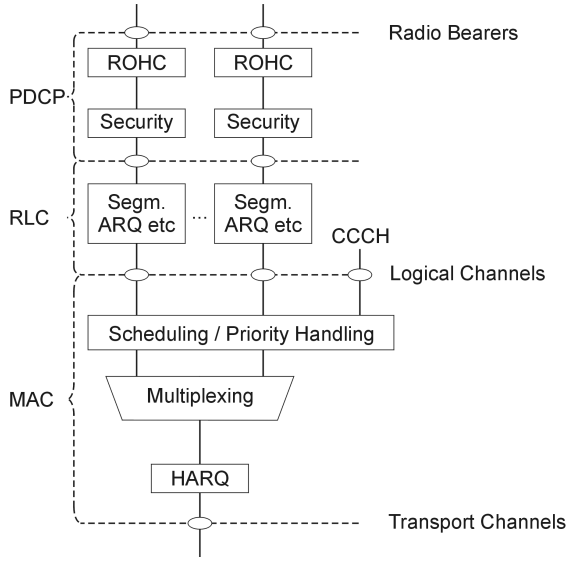


Figure 1.85 Layer 2 structure for UL (TS36.300). Reproduced with permission from © 3GPP™.

channels. Logical channels are used by higher layers to differentiate between logical connections which may use different metrics, for example, in terms of quality or delay, and so on. Furthermore, logical channels are used to distinguish control plane connections, either CCCHs or DCCHs, from user plane connections (DTCHs).

Table 1.20 Values of LCID for DL-SCH. Reproduced with permission from © 3GPP™

Index	LCID values
00000	CCCH
00001–01010	Identity of the logical channel
01011–11011	Reserved
11100	UE contention resolution identity
11101	Timing advance command
11110	DRX command
11111	Padding

Table 1.21 Values of LCID for UL-SCH. Reproduced with permission from © 3GPP™

Index	LCID values
00000	CCCH
00001–01010	Identity of the logical channel
01011–11001	Reserved
11010	Power headroom report
11011	C-RNTI
11100	Truncated BSR
11101	Short BSR
11110	Long BSR
11111	Padding

Services provided by the physical layer to the MAC layer are granted via another type of SAP. SAPs between the MAC and the physical layer are transport channels. Transport channels match data units to physical channels in which data is supposed to be transmitted. One exception is the PCH which is multiplexed into the PDSCH identified with the P-RNTI = 0xFFFE.

Multiplexing of data units from logical channels to transport channels is one of the tasks of the MAC layer. Logical channels are differentiated with LCIDs. Tables 1.20 and 1.21 show the defined LCIDs and their values for DL and UL respectively. A CCCH always has LCID = 0. Other UE dedicated channels start with LCID = 1.

A MAC PDU consists of a MAC payload part and a MAC header part. The MAC payload conveys multiple units of MAC control elements and MAC SDUs from higher layers. Therefore, the MAC header is also divided into sub-headers depending on the units carried in the MAC payload as MAC sub-headers describe the MAC payload units. There are various possible combinations of MAC control elements, MAC SDUs, and MAC padding derivatives. An example of a MAC PDU with a combination of MAC sub-headers, MAC control elements, and MAC SDUs in the payload section is depicted in Figure 1.86.

Logical channels which are multiplexed to transport channels are prioritized by the scheduling algorithm. The scheduling algorithm decides what to schedule on which physical resources as described in detail for DL scheduling in Section 1.8.6 and UL scheduling in Section 1.8.9. There is only one MAC entity per UE; thus, the UL within the UE has one MAC entity and the eNB executes multiple parallel MAC entities in the DL direction in case the eNB has to handle multiple UEs (as seen in Figures 1.84 and 1.85).

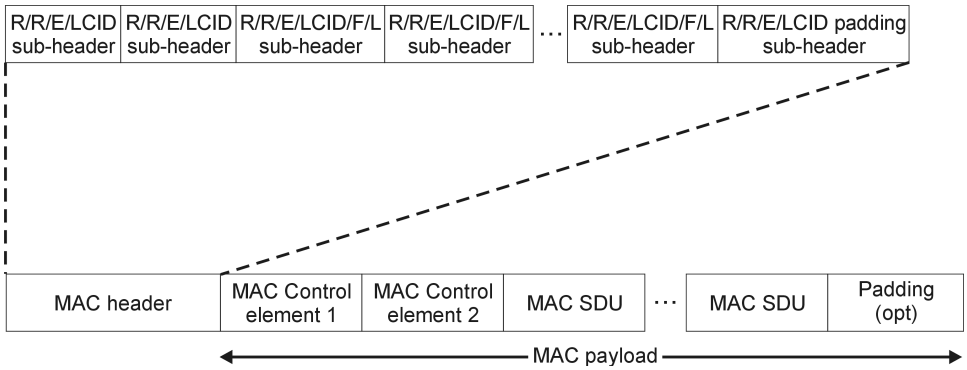


Figure 1.86 Example of MAC PDU consisting of MAC header, MAC control elements, MAC SDUs, and padding (TS36.321). Reproduced with permission from © 3GPP™.

The MAC layer implements a soft combining N-process stop-and-wait FEC and detection mechanism, or HARQ (Hybrid Automatic Repeat Request). Transport blocks are protected with a FEC algorithm known as turbo codes. Soft combining means not correctly decoded blocks are not acknowledged in order to conduct a retransmission, but the previous received not decoded block is held in a soft buffer to be recombined with the new retransmission. This process of soft combining two or more receptions increases the chance that the last received retransmission can be decoded error-free.

1.10.6 Radio Link Control (RLC) Protocol

The RLC layer uses SAPs of the MAC layer which are logical channels. Those SAPs are used to induct its RLC PDUs from the RLC entities. The RLC layer instead provides basically three types of SAPs to the PDCP layer above the RLC layer. The SAPs provide access to the three operating modes to convey data PDUs, either the control plane or user plane: Transparent Mode (TM), Unacknowledged Mode (UM), and Acknowledged Mode (AM). Basic operating entities of the RLC layer are depicted in Figure 1.87.

1.10.6.1 RLC Transparent Mode (TM)

The TM transmits PDUs from the upper layer transparently, which means that the RLC layer is basically just storing and forwarding those PDUs. No feedback is requested on whether the data units were delivered or not. Furthermore, packets are transparently forwarded by keeping them at the same size.

Figure 1.88 illustrates a transmitting and a receiving RLC TM entity.

The TM is used to transmit cell-wide channels as UE paging and the broadcast of system information. It is a typical mode for point-to-multipoint connections without any feedback from receivers. Additionally, CCCHs (LCID = 0) are sent by using the RLC TM.

1.10.6.2 RLC Unacknowledged Mode (UM)

In contrast to the TM, the UM adds segmentation and concatenation of PDUs. This processing step fits higher layer PDUs to the current available transport block size indicated by lower layers.

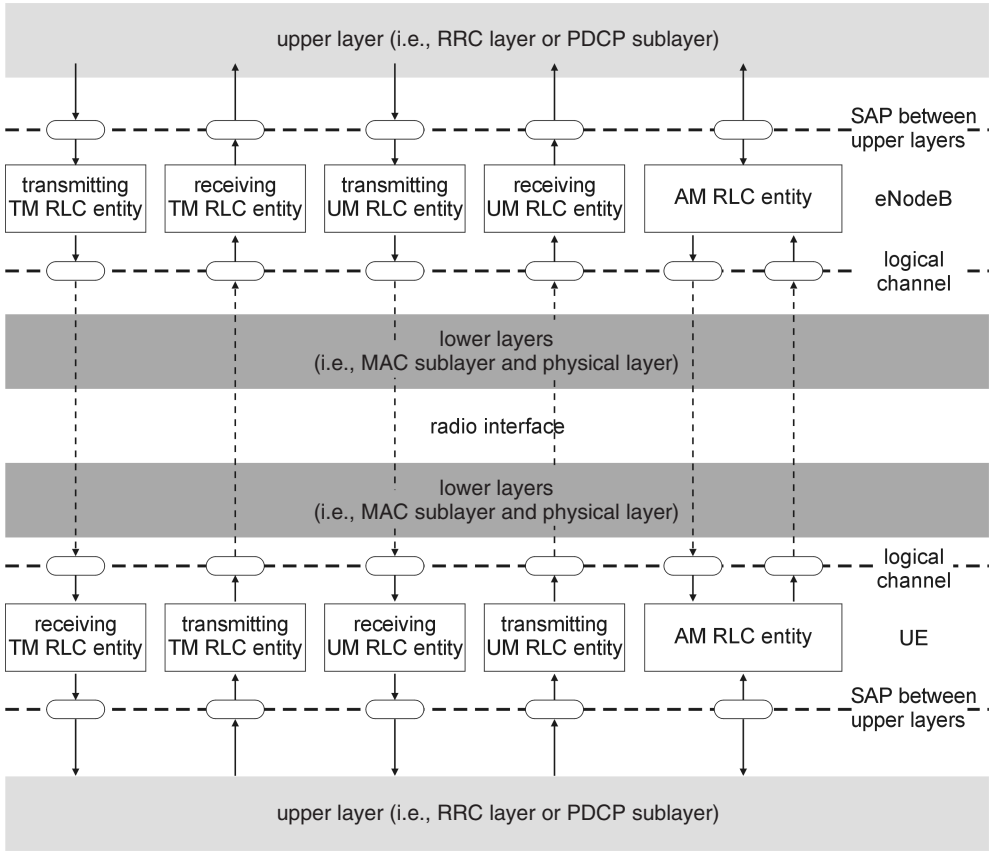


Figure 1.87 RLC layer overview with TM, UM, and AM RLC entities. Reproduced with permission from © 3GPP™.

Segmentation reduces the size of PDUs by splitting them apart. Figure 1.89 illustrates the segmentation of PDCP SDUs.

Concatenation instead is merging PDCP SDUs to a larger RLC PDU. Figure 1.90 depicts this process of building longer PDUs, again in order to decrease padding (adding zeros at the end of a PDU) and use large transport blocks more efficiently.

As the name already indicates, the UM (Figure 1.91) does not request feedback from the peer RLC entity within the receiver, like ACKs of received packets. The UM is used for point-to-point connections and uses error protection of the MAC layer which uses HARQ. But on the RLC level no retransmission process is enabled in UM transmissions. Some higher layer radio bearers allow rare packet loss, for example, IP/UDP traffic or IP/TCP traffic which is taking care of lower layer packet loss with its own retransmissions on the application level.

1.10.6.3 RLC Acknowledged Mode (AM)

Although the MAC layer uses the enabled HARQ procedure with the UM, it is still possible that packets will get lost between RLC peer entities. This could, for example, occur when the maximum

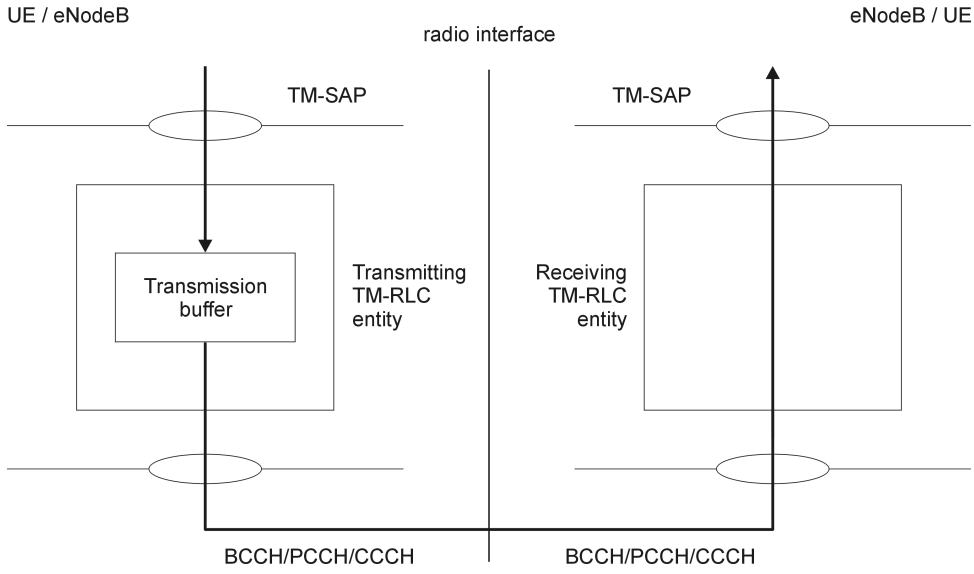


Figure 1.88 Model of two Transparent Mode peer entities. Reproduced with permission from © 3GPP™.

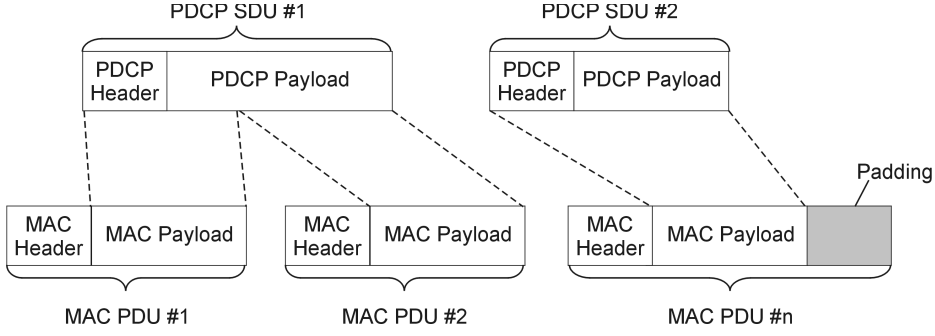


Figure 1.89 Example of RLC segmentation of PDCP SDUs into MAC PDUs. The MAC Payload is equivalent to RLC PDUs.

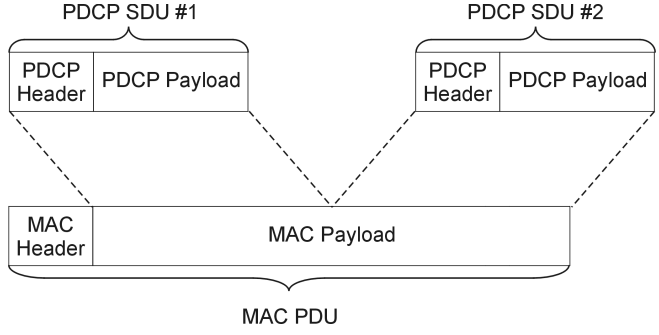


Figure 1.90 Example of RLC concatenation of several PDCP SDUs into one MAC PDU.

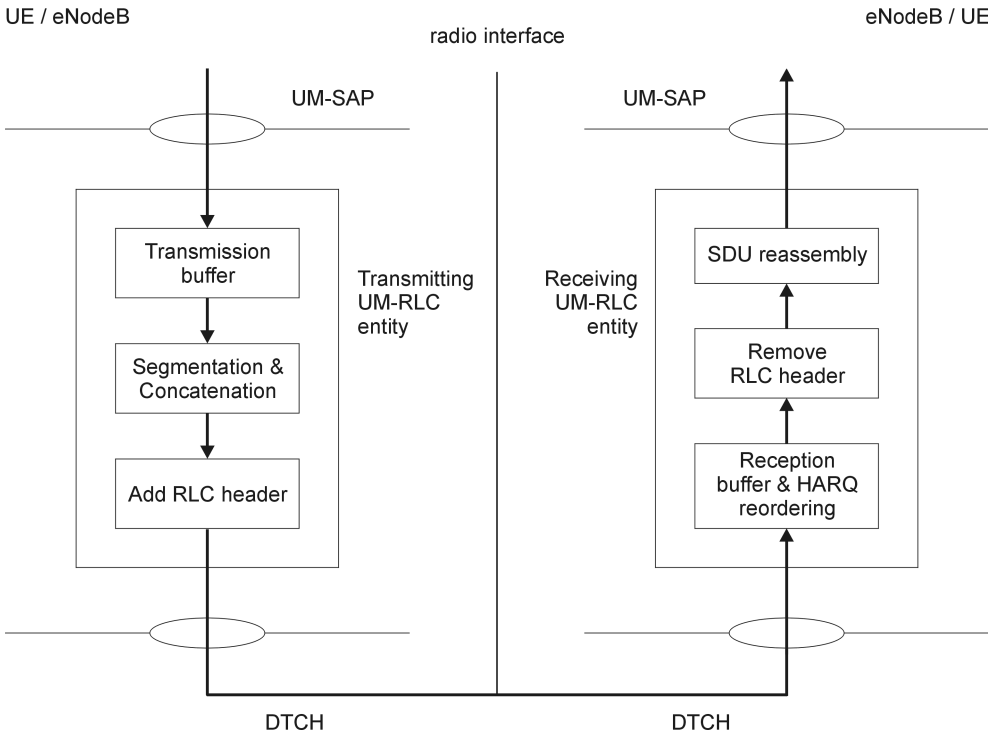


Figure 1.91 Model of two Unacknowledged Mode peer entities. Reproduced with permission from © 3GPP™.

number of retransmissions of the HARQ process is reached. Thus, the AM introduces a secondary outer loop ARQ with ACK feedback from the receiving RLC entity in order to conduct retransmissions of lost packets. Two stacked ARQ loops, fast retransmissions of HARQ, and the outer loop ARQ of the RLC AM lead to good protection for point-to-point DTCHs or DCCHs (used, for example, for RRC and NAS packets).

Furthermore, segmentation and concatenation are applied with the AM as with the UM in order to fit PDU sizes. Figure 1.92 illustrates RLC entities in the AM with the information flow through the different functions.

1.10.7 Packet Data Convergence Protocol (PDCP)

Located above the RLC layer is the PDCP layer. The PDCP layer provides direct data transport for control plane messages (RRC and NAS) and for user plane packets. User plane packets are application layer IP packets as LTE defines only packet-based (IP) data communication. Thus, voice or video service is always IP based (VoIP).

SAPs above the PDCP layer are radio bearers which are mapped to TM, UM, or AM SAPs of the RLC layer below. Figure 1.93 depicts the systematic functions and services of the PDCP layer.

Sequence numbering ensures in-sequence delivery of SDUs for the user plane and control plane of disordered delivered packets of lower layers. Different sequence number lengths are defined: 5, 7, and 12 bits. The 5-bit sequence numbers are reserved for Signaling Radio Bearers (SRBs) carrying

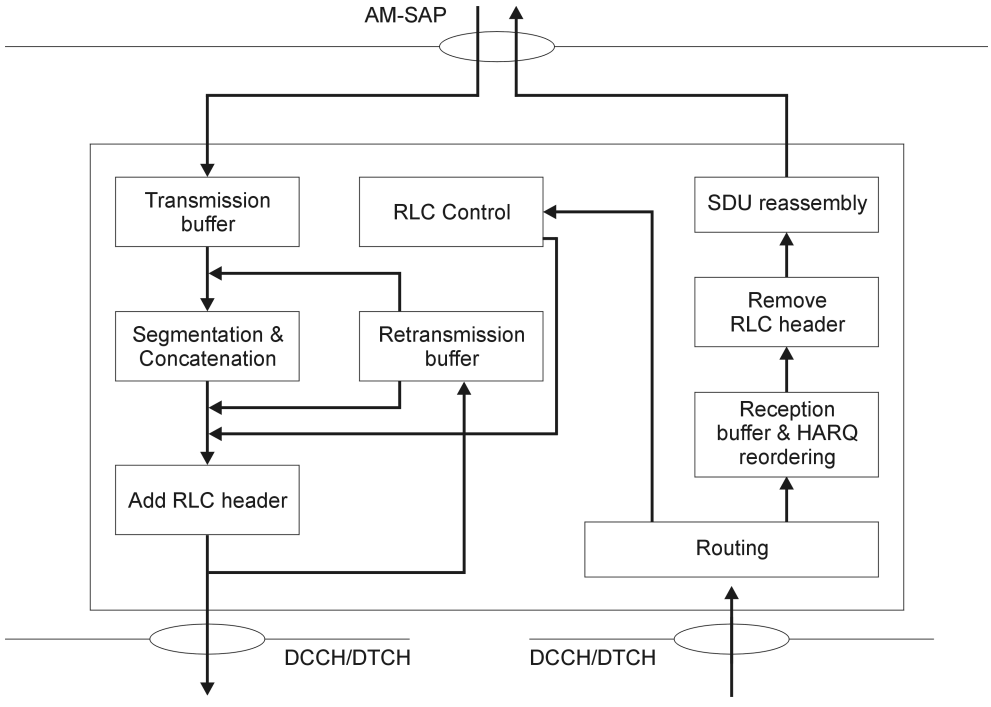


Figure 1.92 Model of an Acknowledged Mode entity. Reproduced with permission from © 3GPP™.

control plane SDUs only. The 7-bit and 12-bit sequence numbers are dedicated to Dedicated Radio Bearers (DRBs) conveying user plane SDUs with application layer IP data.

Header compression is a feature for user plane transmission in order to decrease application header overhead and to increase overall efficiency. Application headers as IP headers are used for network routing and can be compressed on such air interface point-to-point transmission links. The header overhead is especially large when small packets are used, for example, with VoIP where, besides the IP and UDP header, also an RTP header is in front of the payload.

Only the Robust Header Compression (RoHC) algorithm is applied with LTE. RoHC is defined by the Internet Engineering Task Force (IETF). Several RFCs (describing profiles and protocols of the IETF) can be used with LTE. Table 1.22 lists the 10 defined RoHC profiles which are permitted to be used.

Furthermore, integrity protection for the control plane, thus for SRBs, is a function of PDCP as well as ciphering and deciphering functionality.

The format of a PDCP Data PDU for the transport of SRB control plane information is shown in Figure 1.94. Besides the data field with higher layer protocol information, there is a PDCP sequence number, some reserved spare bits, and four octets for the integrity protection message authentication code (MAC-I).

For user plane transport, there are two different formats of PDCP PDUs defined: one with a long 12-bit PDPC sequence number and one with a short 7-bit sequence number (shown in Figure 1.95). The long sequence number format is used for transporting RLC AM and UM information, the short sequence number format for transporting RLC TM frames. The sequence number length for transporting SRB frames is 5 bits.

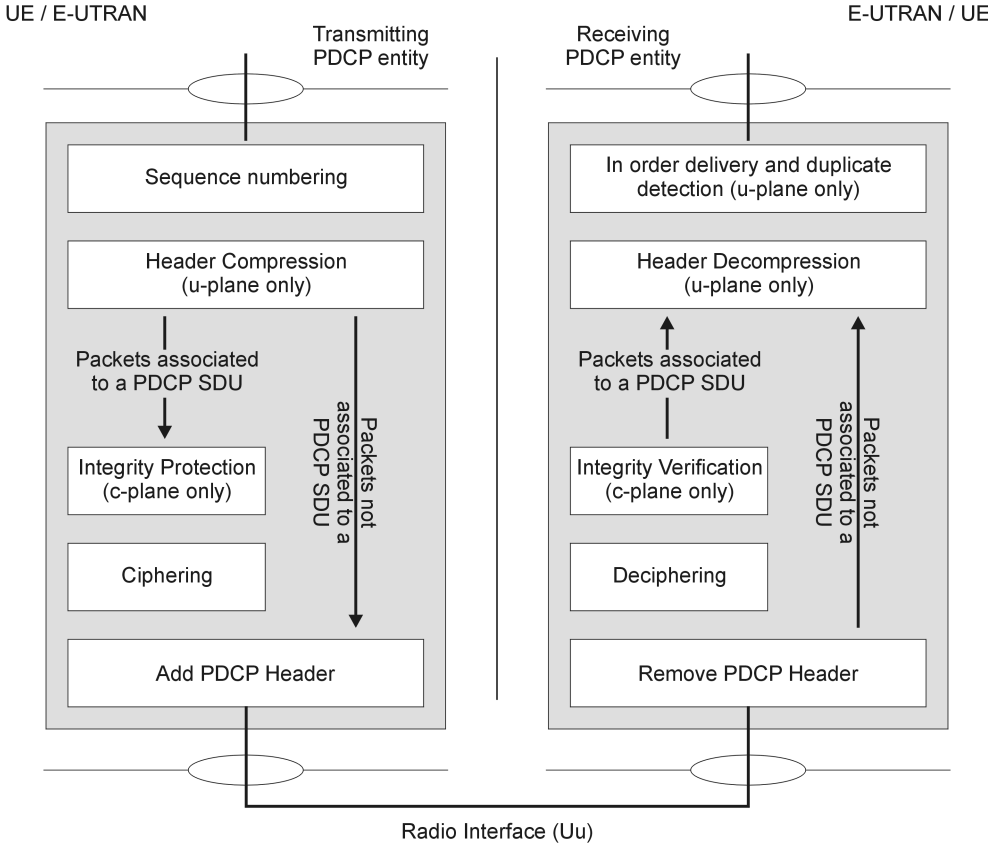


Figure 1.93 Functional overview of the PDCP layer (TS36.323). Reproduced with permission from © 3GPP™.

Table 1.22 Supported header compression protocols and profiles. Reproduced with permission from © 3GPP™

Profile identifier	Usage	Reference
0x0000	No compression	RFC 4995
0x0001	RTP/UDP/IP	RFC 3095, RFC 4815
0x0002	UDP/IP	RFC 3095, RFC 4815
0x0003	ESP/IP	RFC 3095, RFC 4815
0x0004	IP	RFC 3843, RFC 4815
0x0006	TCP/IP	RFC 4996
0x0101	RTP/UDP/IP	RFC 5225
0x0102	UDP/IP	RFC 5225
0x0103	ESP/IP	RFC 5225
0x0104	IP	RFC 5225

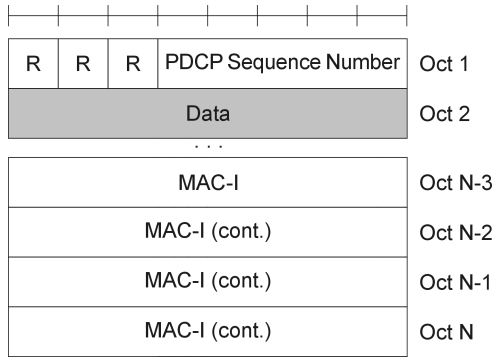


Figure 1.94 Format of PDCP data PDU for transport of signaling radio bearer information. Reproduced with permission from © 3GPP™.

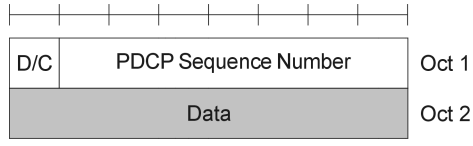


Figure 1.95 Format of PDCP data PDU for transport of user plane information. Reproduced with permission from © 3GPP™.

The D/C field is used to distinguish between user plane (D) and control plane (C) data carried by PDCP.

1.10.8 Radio Resource Control (RRC) Protocol

The RRC protocol is responsible for the setup, reconfiguration, and release of the radio interface connection. This includes the setup, modification, and release of SRBs, default and dedicated radio bearers, along with the necessary QoS control and initial security activation. Also the paging of UEs to request establishment of mobile terminated connections is a function of RRC. To provide network-specific access parameters, RRC system information is broadcasted by all cells of the network. The UE uses RRC to report a set of various measurements to the eNB. Some of these measurement reports can trigger intra-LTE or inter-RAT handover and RRC is in charge of all these mobility procedures. As a special function that is required to support the best possible "always-on" scenario, RRC comes with an error recovery function that allows a dropped RRC connection to be re-established quickly. Similar functionality, called RRC re-establishment, was introduced with RRC used in 3G UTRAN.

Although the functions of LTE RRC are almost the same as for 3G UTRAN RRC, far fewer signaling messages have been defined for LTE RRC. So at first sight LTE RRC looks simpler. The trick used by the standard definition group is that it has defined only dedicated messages for RRC connection setup, release, reconfiguration, and re-establishment, but in fact the LTE RRC reconfiguration procedure is a very complex process that combines all functions covered by the 3G UTRAN RRC protocol procedures, namely physical channel reconfiguration, transport channel reconfiguration, radio bearer

setup, radio bearer reconfiguration, radio bearer release, and RRC measurement control. Consequently, it is now very difficult in LTE to find out what exactly is reconfigured.

1.10.8.1 RRC States

In contrast to 3G UMTS where four different RRC states have been defined, LTE recognizes only two RRC states, which means that the radio connection between the UE and network can be either active or not active (as was known from GSM).

In the RRC_IDLE state the radio connection is inactive. The UE mobility is not under control of the network and the UE does not need to send any measurement reports for updating, although it performs neighbor cell measurement for cell (re)selection. However, the UE monitors the PCH to detect incoming calls and it also monitors system information broadcast on the BCCH. This is the most important part of the system information, typically the MIB, since in LTE the larger part of system information is not signaled on the BCH but on the DL-SCH.

In the RRC_CONNECTED state the UE is able to send and receive data in the UL and DL direction. It measures the DL radio quality of neighbor cells and sends RRC measurement reports according to the measurement configuration received from the MME. However, it is the eNodeB, and the MME, that are respectively in charge of making handover decisions and triggering handover execution when necessary. The UE continues to monitor the PCH to detect incoming calls. In the RRC_CONNECTED mode all system information sent on the DL-SCH, especially SIB 1 which contains information about change of system parameters, is readable by the UE.

When it is necessary to perform inter-RAT mobility, there will be a transition from LTE RRC states to UTRA or GSM states as illustrated in Figure 1.96.

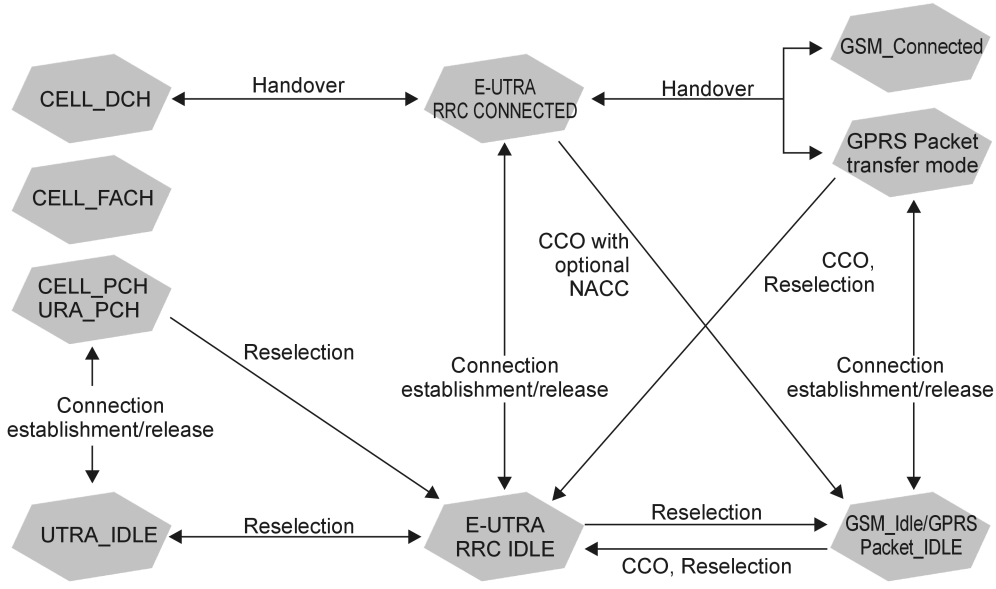


Figure 1.96 RRC state transitions in case of inter-RAT mobility. Reproduced with permission from © 3GPP™.

When changing the RAT in the IDLE mode, this will always happen on account of reselection, which means the UE measures the radio quality of the available radio access technologies and selects the best suitable to log in and register to the network. This procedure also applies for UEs in the CELL_PCH and URA_PCH states in the 3G UTRAN. In the CELL_PCH or URA_PCH state, there is no active radio connection between the UE and network, but RRC context information stored in the RNC, and the state transition from CELL_PCH/URA_PCH to E-UTRA IDLE, mean that a UE in CELL_PCH is allowed without further notice to change the E-UTRAN.

A handover from E-UTRA RRC CONNECTED to 3G UMTS will see the UE enter 3G UMTS in the CELL_DCH state, and a handover to the GERAN starting from the E-UTRA RRC CONNECTED state will end up in the GSM_CONNECTED state for voice services after CS Fallback or GPRS packet transfer mode for non-real-time PS services. It is also possible that the UE is ordered to execute a Cell Change Order (CCO) from E-UTRA RRC CONNECTED to GSM_IDLE/GPRS Packet_IDLE or from GPRS packet transfer mode to E-UTRA RRC IDLE. In case of such a CCO, the UE must – as in the case of reselection – establish a radio connection and register at the network (e.g., with combined Routing/LA Update) before the user plane payload can be transferred under the umbrella of a still active PDP context. To minimize the delay for this registration procedure, which may take up to 10 seconds, the Network Assisted Cell Change (NACC) was introduced in 3GPP 44.901.

1.10.8.2 System Information

System information is divided into the MIB and a number of SIBs. The MIB includes the DL transmission bandwidth and the PHICH information of the broadcasting cell. The MIB is transmitted on the BCH (transport), that is, mapped onto the PBCH. The MIB is the only system information sent on the BCH. All other SIBs are transmitted using the DL-SCH.

To find the RBs that carry SIBs on the DL-SCH, a SI-RNTI is signaled on the PDCCH. The SI-RNTI indicates in which RBs the SIB *Type1* can be found.

The MIB and SIB 1 are sent periodically (MIB periodicity: 40 ms, SIB 1 periodicity: 80 ms); all other system information messages are flexibly scheduled.

SIB 1 (see Message Example 1.1) contains the PLMN identity, tracking area code, and CI of the broadcasting cell. It also contains Q-RxLevMin, which is the minimum RSRP threshold that a broadcasting cell should be measured with before initial cell selection, and later one random access is performed by the UE. There is also SIB Mapping Info included to inform the UE which SIBs are transmitted and how they are scheduled. Furthermore, the MAC decoder output of Message Example 1.1 shows the SI-RNTI and transport/physical channel used to transmit SIB 1.

Message Example 1.1: SIB 1

```
+-----------------------------------------------------+-----------------------------------------+
|ID Name                                              |Comment or Value                         |
+-----------------------------------------------------+-----------------------------------------+
|56  05:43:34,555,032  RRC-UU    K2AIR-PHY  PDSCH  LTE-RLC/MAC  MAC-TM-PDU (DL)  LTE-RRC_BCCH_DL_SCH
systemInformationBlockType1                 |
|Tektronix K2Air LTE PHY Data Message Header (K2AIR-PHY)  PDSCH (= PDSCH Message)                  |
|1 PDSCH Message                                                                                   |
|1.1 Common Message Header                                                                         |
|Protocol Version                                     |0                                        |
|Transport Channel Type                               |DL-SCH                                   |
|Physical Channel Type                                |PDSCH                                    |
|System Frame Number                                  |454                                      |
|Direction                                            |Downlink                                 |
|Radio Mode                                           |FDD                                      |
|Internal use                                         |0                                        |
|Status                                               |Original data                            |
```

```
|Reserved                                          |0                                                  |
|Physical Cell ID                                  |0                                                  |
|UE ID/RNTI Type                                   |SI-RNTI                                            |
|Subframe Number                                   |5                                                  |
|UE ID/RNTI Value                                  |'ffff'H                                            |
|1.2 PDSCH Header                                                                                      |
|CRC report                                        |CRC ok                                             |
|HARQ process number                               |0                                                  |
|Reserved                                          |0                                                  |
|Transport Block Indicator                         |single TB info                                     |
|Reserved                                          |0                                                  |
|1.2.1 Transport Block#1 Information                                                                   |
|Transport Block#1 Size                            |144                                                |
|Modulation Order DL 1                             |QPSK                                               |
|New Data Indicator DL 1                           |new data                                           |
|Redundancy Version DL 1                           |1                                                  |
|Reserved                                          |0                                                  |
|Modulation Scheme Index DL 1                      |5                                                  |
|Reserved                                          |0                                                  |
|1.2.2 Transport Block Data                                                                            |
|TB1 Mac-PDU Data                                  |40 51 00 21 00 00 20 00 10 0c 14 01 10
                                                    21 00 68 22 b6                                    |
|Padding                                           |'0068'H                                            |
|1.3 Additional Call related Info                                                                      |
|Number Of Logical Channel Informations            |1                                                  |
|1.3.1 Logical Channel Information                                                                     |
|LCID                                              |0                                                  |
|RLC Mode                                          |Transparent Mode                                   |
|Radio Bearer ID                                   |0                                                  |
|Radio Bearer Type                                 |Control Plane (Signalling)                         |
|Spare                                             |0                                                  |
|Spare                                             |0                                                  |
|Logical Channel Type                              |BCCH                                               |
|Call ID                                           |'fffffff5'H                                        |
|3GPP LTE-RLC/MAC Rel.8 (MAC TS 36.321 V8.5.0, 2009-03, RLC  TS 36.322 V8.5.0, 2009-03) (LTE-RLC/
MAC)  MAC-TM-PDU (DL) (= MAC PDU (Transparent Content Downlink))  |
|1 MAC PDU (Transparent Content Downlink)                                                              |
|MAC Transparent Data                              |40 51 00 21 00 00 20 00 10 0c 14 01 10
                                                    21 00 68 22 b6                                    |
|RRC (BCCH DL SCH)  3GPP TS 36.331 V8.5.0 (2009-03) (LTE-RRC_BCCH_DL_SCH)
systemInformationBlockType1 (= systemInformationBlockType1)  |
|bCCH-DL-SCH-Message                                                                                   |
|1 message                                                                                             |
|1.1 Standard                                                                                          |
|1.1.1 systemInformationBlockType1                                                                     |
|1.1.1.1 cellAccessRelatedInfo                                                                         |
|1.1.1.1.1 plmn-IdentityList                                                                           |
|1.1.1.1.1.1 pLMN-IdentityInfo                                                                         |
|1.1.1.1.1.1.1 plmn-Identity                                                                           |
|1.1.1.1.1.1.1.1 mcc                                                                                   |
|1.1.1.1.1.1.1.1.1 mCC-MNC-Digit                   |2                                                  |
|1.1.1.1.1.1.1.1.2 mCC-MNC-Digit                   |9                                                  |
|1.1.1.1.1.1.1.1.3 mCC-MNC-Digit                   |9                                                  |
|1.1.1.1.1.1.1.2 mnc                                                                                   |
|1.1.1.1.1.1.1.2.1 mCC-MNC-Digit                   |0                                                  |
|1.1.1.1.1.1.1.2.2 mCC-MNC-Digit                   |0                                                  |
|1.1.1.1.1.1.2 cellReservedForOperatorUse          |notReserved                                        |
|1.1.1.1.2 trackingAreaCode                        |'0000'H                                            |
|1.1.1.1.3 cellIdentity                            |'2000100'H                                         |
|1.1.1.1.4 cellBarred                              |notBarred                                          |
|1.1.1.1.5 intraFreqReselection                    |notAllowed                                         |
```

```
|1.1.1.1.6 csg-Indication                    |false                                    |
|1.1.1.2 cellSelectionInfo                                                             |
|1.1.1.2.1 q-RxLevMin                        |-65                                      |
|1.1.1.3 freqBandIndicator                   |1                                        |
|1.1.1.4 schedulingInfoList                                                            |
|1.1.1.4.1 schedulingInfo                                                              |
|1.1.1.4.1.1 si-Periodicity                  |rf16                                     |
|1.1.1.4.1.2 sib-MappingInfo                                                           |
|1.1.1.4.2 schedulingInfo                                                              |
|1.1.1.4.2.1 si-Periodicity                  |rf32                                     |
|1.1.1.4.2.2 sib-MappingInfo                                                           |
|1.1.1.4.2.2.1 sIB-Type                      |sibType3                                 |
|1.1.1.4.2.2.2 sIB-Type                      |sibType6                                 |
|1.1.1.4.3 schedulingInfo                                                              |
|1.1.1.4.3.1 si-Periodicity                  |rf32                                     |
|1.1.1.4.3.2 sib-MappingInfo                                                           |
|1.1.1.4.3.2.1 sIB-Type                      |sibType5                                 |
|1.1.1.5 si-WindowLength                     |ms20                                     |
|1.1.1.6 systemInfoValueTag                  |22                                       |
```

SIB 2 contains timers and constants, barring information, UL frequency information, and UL bandwidth information. SIB 3 contains parameters for the cell reselection procedure. SIB 4 contains neighbor cell information for intra-frequency cell reselection. SIB 5 contains information for inter-frequency cell reselection. SIB 6 contains information for inter-RAT cell reselection to the UTRAN. SIB 7 contains information for inter-RAT cell reselection to the GERAN. SIB 8 contains information for inter-RAT cell reselection to CDMA2000. SIB 9 is used to broadcast the home eNB name (HNB name). SIB 10 and SIB 11 can be used to broadcast warning information to subscribers (e.g., tsunami warnings).

1.10.8.3 RRC Measurements

As in 3G UTRAN, the RRC measurement reports are expected to be sent mostly as event-triggered reports. The events listed in Table 1.23 have been specified so far (3GPP 36.331 v.8.9.0 2010-03).

The thresholds mentioned in the event description refer either to RSRP or RSRQ measurements. This is specified when the measurement is set up. To ensure that only significant changes of the radio quality are reported, the measurements are guarded with the additional parameters of hysteresis, offset, and time-to-trigger. The hysteresis parameter is used to eliminate ping-pong effects in measurement reporting as shown in Figure 1.97. Here the events A1 and A2 will only be reported for the serving cell measured by UE 1, but not for the serving cell of UE 2.

Table 1.23 RRC measurement event IDs and description

Event ID	Description
A1	Serving becomes better than threshold
A2	Serving becomes worse than threshold
A3	Neighbor becomes offset better than serving
A4	Neighbor becomes better than threshold
A5	Serving becomes worse than threshold 1 and neighbor becomes better than threshold 2
B1	Inter-RAT neighbor becomes better than threshold
B2	Serving becomes worse than threshold 1 and inter-RAT neighbor becomes better than threshold 2

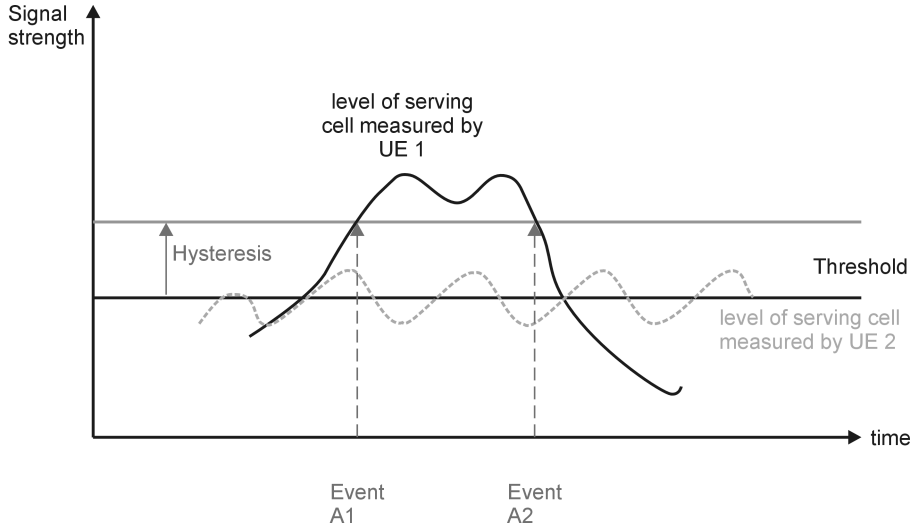


Figure 1.97 Hysteresis parameter for RRC measurements.

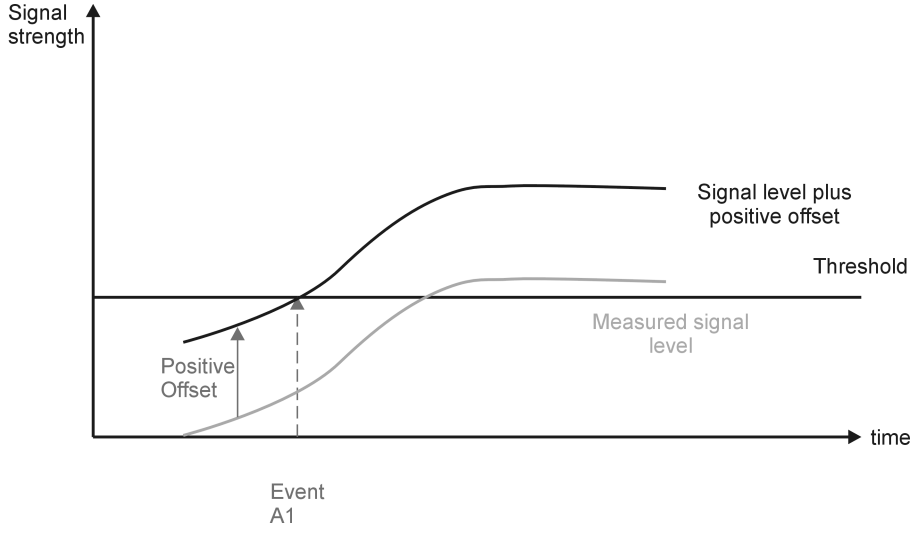


Figure 1.98 Offset parameter for RRC measurements.

The offset parameter (see Figure 1.98) is not related to a predefined threshold, like hysteresis, but to the actual measurement result. The offset can have positive or negative values. The purpose of using the offset parameter is to speed up or slow down handover in/from strong/weak cells.

Time-to-trigger should prevent short-time peaks of measured signals from triggering measurement reports and subsequent handover procedures. Looking at Figure 1.99, the setting of the time-to-trigger parameter prevents a handover to cell 2, where the radio quality would have dropped quickly back to below the required threshold. Instead the call can be handed over to cell 1 after A1's report is

Ex.1013.00120

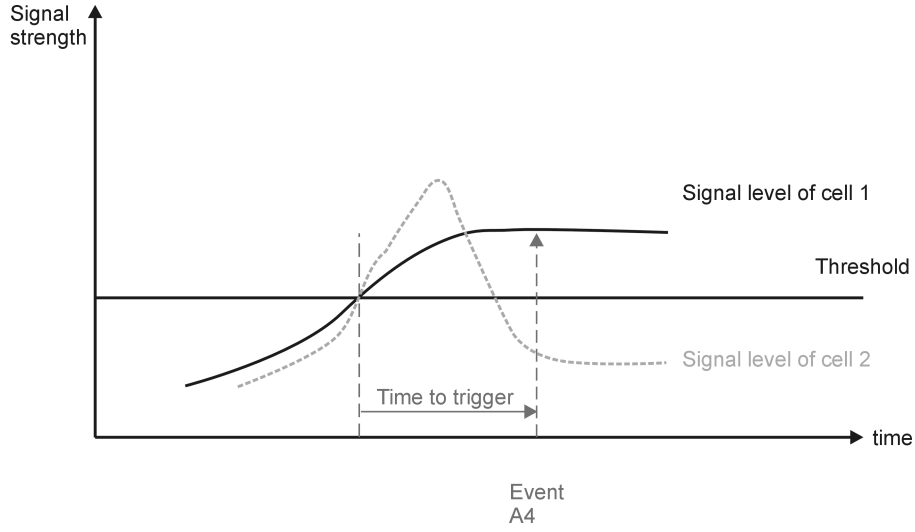


Figure 1.99 Time-to-trigger parameter for RRC measurements.

sent, knowing that cell 1 offers not just a radio quality above the required threshold, but also stable radio conditions.

1.10.9 Non-Access Stratum (NAS) Protocol

1.10.9.1 EPS Mobility Management and Connection Management States

On the NAS layer there are two EPS Mobility Management (EMM) states defined to describe the results of mobility management procedures like Attach and Tracking Area Update. The EMM states are:

- EMM-DEREGISTERED.
- EMM-REGISTERED.

The UE in the EMM-DEREGISTERED state is not attached to the network. From the MME's point of view, there is no active context for a UE, no routing information, and no location information.

After a successful attach the UE enters the EMM-REGISTERED state. Now the MME knows where to page the UE and the HSS is able to provide routing information for mobile terminating connections of this particular subscriber. In the EMM-REGISTERED state the UE always has an active PDN connection and EPS security context.

The ECM states indicate if there is an active signaling connectivity between the UE and the EPC. The ECM states are:

- ECM-IDLE.
- ECM-CONNECTED.

The location of a UE in the ECM-IDLE state is known by the network on behalf of the current Tracking Area List. This list contains all tracking areas for which the UE performed successful initial registration (attach) to the network and subsequent successful tracking area update procedures. All

tracking areas in a Tracking Area List to which a UE is registered must be connected to the same MME (according to 3GPP 23.401).

A UE is in the ECM-IDLE state when no active NAS signaling connection between the UE and network exists. In other words, there are no SRBs assigned to this mobile. If the UE changes its geographic position it may perform cell selection/reselection when necessary.

The UE and MME should enter the ECM-CONNECTED state whenever the UE sends or MME receives one of the following NAS messages: Attach Request, Tracking Area Update Request, Service Request, or Detach Request.

When the UE is in the ECM-IDLE state it is possible that the UE and the network have different sets of established EPS bearers stored in their system memory. When the UE and MME enter the ECM-CONNECTED state, the set of EPS bearers is synchronized between the UE and network.

ECM state and EMM state do not strictly depend on each other. For instance, a UE can be in ECM-IDLE, but EMM-REGISTERED. However, a UE can also be in ECM-CONNECTED while in EMM-DEREGISTERED, yet this happens during the radio connection for initial registration. Firstly, the UE must enter ECM-CONNECTED to send Attach Request, and only if Attach Accept is sent back by the network does this UE enter EMM-REGISTERED.

1.10.10 S1 Application Part (S1AP)[6]

The S1AP is used for the protocol dialog between the MME and eNB. Here its first function is to establish a relation between these two network elements, known in the protocol standard document as the S1 setup procedure. A set of S1AP management messages is further used to maintain this connection, change configuration parameters, indicate possible errors and overload situations, balance the load, and reset, re-establish, or release the connection.

Once the relation between the eNB and MME is successfully established, UEs camping on the cells of this eNB can be paged using the S1AP to establish mobile terminating connections or can register and set up mobile originating calls by themselves. In the case of such a registration of connection setup procedure, the S1AP provides functions for transparent forwarding of NAS messages. During connection setup the S1AP is in charge of the tunnel management of S1-U GTP tunnels. Using the S1AP signaling procedure, these S1 user plane tunnels can be established, modified according to changing QoS parameters, and released. The S1-U GTP tunnels are part of the E-RAB and in fact it is the S1AP that provides full E-RAB management functions. Setup and modification of E-RABs are always triggered by the MME, while the release of E-RABs can be triggered by both the MME and eNB.

In using the S1AP during initial registration and connection setup, an S1 UE context is established in the eNB. Each S1AP connection related to a particular UE is identified by a pair of MME UE S1AP ID and eNB UE S1AP ID. These connection identifiers link all S1AP messages belonging to a single subscriber except paging messages (i.e., sent before the UE context is established). Table 1.24 shows the occurrence of the UE S1AP IDs in the different UE-related messages of this protocol.

Messages that are used to establish and maintain the relation between the MME and eNB on the network element level, like the messages of the S1 setup procedure, do not contain any UE ID.

As can be seen in Table 1.24, the S1AP is also responsible for different mobility functions. Belonging to this category is the path switch procedure, that is, a handover between eNBs connected to the same MME. Inter-MME handover and inter-RAT handover are executed using the set of S1AP handover messages – for more details on this topic see Chapter 2 in this book.

E-RABs can be set up, modified, and released at any time during an active connection. Hence, separate E-RAB management messages are provided by the S1AP.

[6] Parts of this chapter are reproduced with permission from © 3GPP™.

Table 1.24 S1AP UE IDs in UE-related messages

S1-AP UE related messages	MME UE S1AP ID	eNB UE S1AP ID
E-RAB setup Request	×	×
E-RAB setup Response	×	×
E-RAB Modify Request	×	×
E-RAB Modify Response	×	×
E-RAB Release Command	×	×
E-RAB Release Response	×	×
E-RAB Release Indication	×	×
Initial Context Setup Request	×	×
Initial Context Setup Response	×	×
Initial Context Setup Failure	×	×
UE Context Release Request	×	×
UE Context Release Command (optionally there is only the MME UE S1AP ID)	×	× (but optional)
UE Context Release Complete	×	×
UE Context Modification Request	×	×
UE Context Modification Response	×	×
UE Context Modification Failure	×	×
Handover Required	×	×
Handover Command	×	×
Handover Preparation Failure	×	×
Handover request	×	No
Handover request acknowledge	×	×
Handover Failure	×	No
Handover Notify	×	×
Path Switch Request	No	×
Path Switch Request acknowledge	×	×
Path Switch Request Failure	×	×
Handover Cancel	×	×
Handover Cancel acknowledge	×	×
eNB Status Transfer	×	×
MME Status Transfer	×	×
Paging	No	No
Initial UE Message	No	×
Uplink NAS Transport	×	×
Downlink NAS Transport	×	×
NAS Non delivery indication	×	×
LOCATION REPORTING CONTROL	×	×
LOCATION REPORT FAILURE INDICATION	×	×
LOCATION REPORT	×	×

In addition, there are messages for the transmission of broadcast warning messages and for location reporting. The S1AP location report will keep the MME update about the ID of the serving cell currently used by the UE.

Looking a little deeper into the protocol details of the S1AP, it emerges that there are two classes of S1AP elementary procedures. Class 1 procedures are characterized by the fact that the initiating message should be answered with a successful or unsuccessful outcome message. The

Table 1.25 S1AP Class 1 elementary procedures. Reproduced with permission from © 3GPP™

Elementary procedure	Initiating message	Successful outcome	Unsuccessful outcome
		Response message	Response message
Handover Preparation	HANDOVER REQUIRED	HANDOVER COMMAND	HANDOVER PREPARATION FAILURE
Handover Resource Allocation	HANDOVER REQUEST	HANDOVER REQUEST ACKNOWLEDGE	HANDOVER FAILURE
Path switch REquest	PATH SWITCH REQUEST	PATH SWITCH REQUEST ACKNOWLEDGE	PATH SWITCH REQUEST FAILURE
Handover Cancellation	HANDOVER CANCEL	HANDOVER CANCEL ACKNOWLEDGE	–
E-RAB SETup	E-RAB SETUP REQUEST	E-RAB SETUP RESPONSE	–
E-RAB MODify	E-RAB MODIFY REQUEST	E-RAB MODIFY RESPONSE	–
E-RAB RELease	E-RAB RELEASE COMMAND	E-RAB RELEASE RESPONSE	–
Initial Context Setup	INITIAL CONTEXT SETUP REQUEST	INITIAL CONTEXT SETUP RESPONSE	INITIAL CONTEXT SETUP FAILURE
Reset	RESET	RESET ACKNOWLEDGE	–
S1 SETUP	S1 SETUP REQUEST	S1 SETUP RESPONSE	S1 SETUP FAILURE
UE Context Release	UE CONTEXT RELEASE COMMAND	UE CONTEXT RELEASE COMPLETE	–
UE Context Modification	UE CONTEXT MODIFICATION REQUEST	UE CONTEXT MODIFICATION RESPONSE	UE CONTEXT MODIFICATION FAILURE
eNB configuration update	ENB CONFIGURATION UPDATE	ENB UPDATE CONFIGURATION ACKNOWLEDGE	ENB CONFIGURATION UPDATE FAILURE
MME Configuration Update	MME CONFIGURATION UPDATE	MME CONFIGURATION UPDATE ACKNOWLEDGE	MME CONFIGURATION UPDATE FAILURE
Write-Replace Warning	WRITE-REPLACE WARNING REQUEST	WRITE-REPLACE WARNING RESPONSE	–

complete list of Class 1 elementary procedures and messages according to 3GPP 36.4313 is given in Table 1.25.

Class 1 elementary procedures are characterized by the fact that each request sent is positively or negatively acknowledged by an appropriate success or failure message.

As known from UTRAN RANAP, there is a difference between message names used in standard documents and encoding of these messages following ASN.1 encoding rules. An example will be

given using the encoding of messages of the handover preparation procedure that is defined in the ASN.1 part of 3GPP 36.413 as follows:

```
handoverPreparation S1AP-ELEMENTARY-PROCEDURE ::= {
    INITIATING MESSAGE  HandoverRequired
    SUCCESSFUL OUTCOME  HandoverCommand
    UNSUCCESSFUL OUTCOME    HandoverPreparationFailure
    PROCEDURE CODE          id-HandoverPreparation
    CRITICALITY     reject
}
```

Translated into a written explanation, this ASN.1 notation means the handover required message will be encoded as Initiating Message with the procedure code = "id-HandoverPreparation," the handover command message will be encoded as Successful Outcome with the procedure code = "id-HandoverPreparation," and Handover Preparation Failure will be encoded as Unsuccessful Outcome with the procedure code = "id-HandoverPreparation."

In contrast to the Class 1 message, the messages of Class 2 are unidirectional messages that are not explicitly acknowledged by the receiving entity. The complete list of Class 2 procedures and messages according to 3GPP 26.314 is given in Table 1.26.

Call scenarios, message examples, and the most important parameters of S1AP messages are described in Chapter 2 of this book.

Table 1.26 S1AP Class 2 elementary procedures. Reproduced with permission from © 3GPP™

Elementary procedure	Message
Handover Notification	HANDOVER NOTIFY
E-RAB Release Request	E-RAB RELEASE REQUEST
Paging	PAGING
Initial UE MEssage	INITIAL UE MESSAGE
Downlink NAS TRansport	DOWNLINK NAS TRANSPORT
Uplink NAS Transport	UPLINK NAS TRANSPORT
NAS non delivery indication	NAS NON DELIVERY INDICATION
Error Indication	ERROR INDICATION
UE Context Release Request	UE CONTEXT RELEASE REQUEST
Downlink S1 CDMA2000 Tunneling	DOWNLINK S1 CDMA2000 TUNNELING
Uplink S1 CDMA2000 Tunneling	UPLINK S1 CDMA2000 TUNNELING
UE Capability Info Indication	UE CAPABILITY INFO INDICATION
eNB Status Transfer	eNB STATUS TRANSFER
MME Status Transfer	MME STATUS TRANSFER
Deactivate Trace	DEACTIVATE TRACE
Trace Start	TRACE START
Trace Failure Indication	TRACE FAILURE INDICATION
Location Reporting Control	LOCATION REPORTING CONTROL
Location Reporting Failure Indication	LOCATION REPORTING FAILURE INDICATION
Location Report	LOCATION REPORT
Overload Start	OVERLOAD START
Overload Stop	OVERLOAD STOP
eNB Direct Information Transfer	eNB DIRECT INFORMATION TRANSFER
MME Direct Information Transfer	MME DIRECT INFORMATION TRANSFER

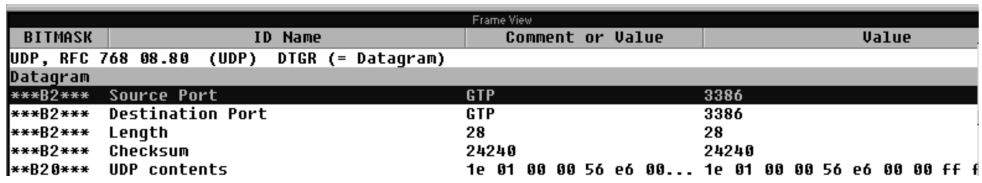


Figure 1.100 UDP datagram.

1.10.11 User Datagram Protocol (UDP)

UDP is a connection-less transport protocol (ISO OSI Model Layer 4), that is, a member of the IP family. UDP is used to transmit higher data quickly from one end of a connection to the other. The source and destination port information elements in the UDP datagram header identify the applications on top of UDP. In the example shown in Figure 1.100 the higher layer application is GTP, so this sample UDP frame is lower layer UDP as can be found on all interfaces of the mobile network that allow tunneling of IP payload.

1.10.12 GPRS Tunneling Protocol (GTP)[7]

GTP is used on various EPC interfaces. Its main functionality is to create, modify, and delete tunnels for IP payload transport. However, besides the tunnel management functionality, the GTP control plane protocol also offers functions and messages for:

- Path management.
- Mobility management.
- CS fallback.
- Non-3GPP-related access.
- Trace management.

Table 1.27 gives an overview of all GTP messages. As in the S1AP we see message pairs of connection-oriented procedures, for instance Create Session Request/Create Session Response. However, there is also a set of connectionless unidirectional messages like Modify Bearer Command.

It should further be noticed that the name of a message often indicates who initiates a connection setup or change of connection parameters. If there is a connection set up by the mobile, the create session procedure will be used to activate the default bearer. If the network requests a bearer establishment it will perform the create bearer procedure. The same differentiation can be seen in the case of bearer modification: a modification requested by the UE side will be performed using the modify bearer procedure; a modification requested by the network is executed using the update bearer procedure.

All in all, the use of GTP on various interfaces in the EPC has the advantage of simplified protocol stacks. This is also an advantage for NEMs, because the implementation effort for network element protocol entity software can be reduced due to the fact that the same or very similar code can be used to program the software, for example, S-GW and PDN-GW. However, for measurement equipment manufacturers like Tektronix Communications the simplified protocol stacks make it harder to track messages of a single connection across multiple interfaces. Additional algorithms in the software

[7] Parts of this chapter are reproduced with permission from © 3GPP™.

Table 1.27 GTP messages. Reproduced with permission from © 3GPP™

Message type value (decimal)	Message	Reference	GTP-C	GTP-U
0	Reserved	–	–	–
1	Echo Request	–	×	×
2	Echo Response	–	×	×
3	Version Not Supported Indication	–	×	–
4–24	Reserved for S101 interface	TS 29.276 [14]	–	–
25–31	Reserved for Sv interface	TS 29.280 [15]	–	–
	SGSN/MME to PGW (S4/S11, S5/S8)			
32	Create Session Request	–	×	–
33	Create Session Response	–	×	–
34	Modify Bearer Request	–	×	–
35	Modify Bearer Response	–	×	–
36	Delete Session Request	–	×	–
37	Delete Session Response	–	×	–
38	Change Notification Request	–	×	–
39	Change Notification Response	–	×	–
40–63	For future use	–	–	–
	Messages without explicit response			
64	Modify Bearer Command (MME/SGSN to PGW – S11/S4, S5/S8)	–	×	–
65	Modify Bearer Failure Indication (PGW to MME/SGSN – S5/S8, S11/S4)	–	×	–
66	Delete Bearer Command (MME to PGW – S11, S5/S8)	–	×	–
67	Delete Bearer Failure Indication (PGW to MME – S5/S8, S11)	–	×	–
68	Bearer Resource Command (MME/SGSN to PGW – S11/S4, S5/S8)	–	×	–
69	Bearer Resource Failure Indication (PGW to MME/SGSN – S5/S8, S11/S4)	–	×	–
70	Downlink Data Notification Failure Indication (**SGSN/**MME to S-GW – S4/S11)	–	×	–
71	Trace Session Activation	–	×	–
72	Trace Session Deactivation	–	×	–
73	Stop Paging Indication	–	×	–
74–94	For future use	–	–	–
	PGW to SGSN/MME (S5/S8, S4/S11)			
95	Create Bearer Request	–	×	–
96	Create Bearer Response	–	×	–
97	Update Bearer Request	–	×	–
98	Update Bearer Response	–	×	–
99	Delete Bearer Request	–	×	–
100	Delete Bearer Response	–	×	–
101–127	For future use	–	–	–
	MME to MME, SGSN to MME, MME to SGSN, SGSN to SGSN (S3/10/S16)			
128	Identification Request	–	×	–
129	Identification Response	–	×	–
130	Context Request	–	×	–

(*continued overleaf*)

Table 1.27 (*continued*)

Message type value (decimal)	Message	Reference	GTP-C	GTP-U
131	Context Response	–	×	–
132	Context Acknowledge	–	×	–
133	Forward Relocation Request	–	×	–
134	Forward Relocation Response	–	×	–
135	Forward Relocation Complete Notification	–	×	–
136	Forward Relocation Complete Acknowledge	–	×	–
137	Forward Access Context Notification	–	×	–
138	Forward Access Context Acknowledge	–	×	–
139	Relocation Cancel Request	–	×	–
140	Relocation Cancel Response	–	×	–
141	Configuration Transfer Tunnel	–	×	–
142–148	For future use	–	–	–
	SGSN to MME, MME to SGSN (S3)			
149	Detach Notification	–	×	–
150	Detach Acknowledge	–	×	–
151	CS Paging Indication	–	×	–
152	RAN Information Relay	–	–	–
153–159	For future use	–	–	–
	MME to S-GW (S11)			
160	Create Forwarding Tunnel Request	–	×	–
161	Create Forwarding Tunnel Response	–	×	–
162	Suspend Notification	–	×	–
163	Suspend Acknowledge	–	×	–
164	Resume Notification	–	×	–
165	Resume Acknowledge	–	×	–
166	Create Indirect Data Forwarding Tunnel Request	–	×	–
167	Create Indirect Data Forwarding Tunnel Response	–	×	–
168	Delete Indirect Data Forwarding Tunnel Request	–	×	–
169	Delete Indirect Data Forwarding Tunnel Response	–	×	–
170	Release Access Bearers Request	–	×	–
171	Release Access Bearers Response	–	×	–
172–175	For future use	–	–	–
	S-GW to SGSN/MME (S4/S11)			
176	Downlink Data Notification	–	×	–
177	Downlink Data Notification Acknowledgement	–	×	–
178	Update Bearer Complete	–	×	–
179–191	For future use	–	–	–
	Other			
192–255	For future use	–	–	–

are necessary to program call trace functions (filter and sequence messages belonging to a single connection) and to correlate performance measurement statistical counters and measurement with the different network elements. In other words, in the past it was quite clear that the GTP-C protocol was only used on the Gn interface between SGSN and GGSN. Now, in EPC, the GTP-C protocol is found on many different interfaces and a bunch of different network elements are using it. Further, a state-of-the-art protocol tester or network monitoring system is required to detect automatically which interfaces and network elements are monitored.

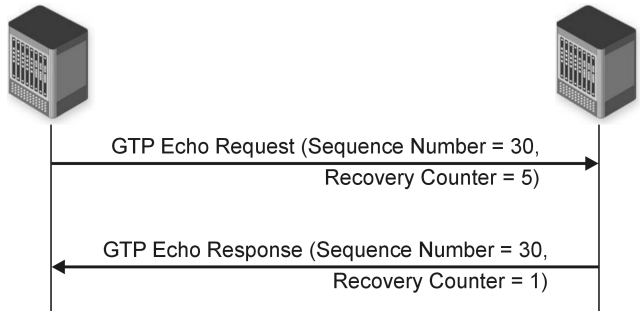


Figure 1.101 GTP path management.

1.10.12.1 Path Management

The path management messages are used to check the activity status of a GTP tunnel on behalf of a heartbeat check mechanism. The messages involved in this procedure are GTP Echo Request and GTP Echo Response as shown in Figure 1.101.

GTP Echo Request is sent with a sequence number that is expected to be received again in an GTP Echo Response sent by the peer entity. The sending of Echo Request is triggered by a timer, but should not happen more often than one Echo Request in 60 seconds for each GTP tunnel.

The functions of the non-3GPP-related access ensure interworking (handover) between E-UTRAN and the CDMA2000 HRDP radio access network.

Trace management is a term that covers all necessary functions to track the activities of selected subscribers. The trace functionality can be used for network element troubleshooting or legal interception.

The path management heartbeat messages are found on both GTP-C and GTP-U connections.

1.10.12.2 Tunnel Management

The create session request message should be sent on the S11 interface by the MME to the S-GW, and on the S5/S8 interface by the S-GW to the PDN GW as part of the procedure:

- E-UTRAN initial attach.
- UE requested PDN connectivity.

The message should also be sent on the S11 interface by the MME to the S-GW in case the S-GW is changed due to mobility. In such cases the create session procedure is embedded in a tracking area update or handover/relocation procedure.

In the create session request message the IMSI is included as a mandatory information element. The network elements on both ends of the GTP-C connection will be identified by their Tunnel Endpoint Identifiers (TEIDs) that during initial assignment are signaled together with the IP addresses of the appropriate network element (see Section 2.2 for more details). Since there will always be a default bearer established when a session is activated, the EPS Bearer ID (EBI) is included as a mandatory information element as well. Together with the TEIDs for the GTP-C signaling connection, a unique triplet of information elements is formed that can always be used to identify a single subscriber's

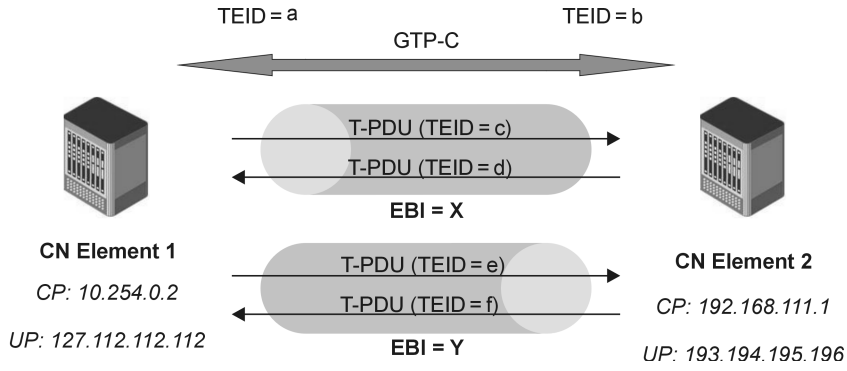


Figure 1.102 GTP tunnel management.

session or bearer unambiguously on any GTP-C interface. The TEIDs are not only used to identify the network elements on both sides of the GTP tunnel, but also used to determine the direction in which the message is sent. This is especially important for monitoring and analyzing user plane traffic.

Figure 1.102 shows the key parameters involved in tunnel management procedures. TEID a and TEID b are used to identify the participating core network elements on the control plane level. EBI X and EBI Y represent two different bearers for the same UE. A maximum of up to 256 bearers per UE is supported. Now, within each bearer there is a unique pair of TEIDs that is used to route the traffic in the UL and DL directions. Since the EBI is only signaled on the control plane, these TEIDs are also used to identify the tunnel established for a particular bearer.

In addition to the differences in TEID parameter values, the IP addresses configured on the transport network layer for user plane and control plane transport are often different as well. However, this is not a standardized setting.

The create bearer request message should be sent on the S5/S8 interface by the PGW (Packet Gateway) to the S-GW and on the S11 interface by the S-GW to the MME as part of the dedicated bearer activation procedure. It contains the EBI as a mandatory information element that links the new dedicated bearer with the previously established session.

If the UE wishes to modify an established bearer, a bearer resource command message should be sent from the MME to the S-GW and forwarded to the PDN-GW. The Bearer Resource Command is triggered by a NAS message with the same name received by the MME. Again it is the EBI information element and the TEIDs that link this.

A bearer resource failure indication should be sent by the PGW to a S-GW and forwarded to the MME to indicate failure of the UE requested bearer resource modification procedure.

The modify bearer request message should only be sent on the S11 interface by the MME to the S-GW and on the S5/S8 interfaces by the S-GW to the PDN GW in case of Tracking Area Update without changing the S-GW, UE-triggered Service Request, or UE.

A DL data notification procedure is used on the S11 interface between the S-GW and the MME to execute the network triggered service request procedure (mobile terminated PS connection request).

The delete indirect data forwarding tunnel request message is sent on the S11 interface by the MME to the S-GW as part of handover procedures.

The Modify Bearer Command should be sent on the S11 interface by the MME to the S-GW, on the S5/S8 interface by the S-GW to the P-GW, and on the S4 interface by the SGSN to the S-GW whenever the subscribed QoS needs to be modified according to QoS information stored in the HSS.

For GTP-based S5/S8, the Update Bearer Request should be sent by the PGW to the S-GW and forwarded to the MME by the following procedures:

- PGW-initiated bearer modification with bearer QoS update.
- HSS-initiated subscribed QoS modification.
- PGW-initiated bearer modification without bearer QoS update.
- UE request bearer resource modification procedure.

The message should also be sent on the S5/S8 interface by the PGW to the S-GW and on the S4 interface by the S-GW to the SGSN as part of the following procedures:

- PGW-initiated EPS bearer modification.
- Execution part of MS-initiated EPS bearer modification.
- SGSN-initiated EPS bearer modification procedure using S4.

A delete bearer command message should be sent on the S11 interface by the MME to the S-GW and on the S5/S8 interface by the S-GW to the PGW as a part of the eNB requested bearer release or MME-initiated dedicated bearer deactivation procedure.

The message should also be sent on the S4 interface by the SGSN to the S-GW and on the S5/S8 interface by the S-GW to the PGW as part of the MS and SGSN-initiated non-default bearer deactivation procedure using S4.

The create indirect data forwarding tunnel request message should be sent on the S11/S4 interface by the MME/SGSN to the S-GW as part of the handover procedures.

The release access bearers request message should be sent on the S11 interface by the MME to the S-GW as part of the S1 release procedure. The message should also be sent on the S4 interface by the SGSN to the S-GW as part of the following procedures:

- RAB release using S4.
- Iu release using S4.

A stop paging indication message should be sent on the S11/S4 interface by the S-GW to the MME/SGSN as part of the network triggered service request procedure.

1.10.12.3 Mobility Management

A forward relocation request message should be sent from the source MME to the target MME over the S10 interface as part of S1-based handover relocation procedure from the source MME to the target SGSN, or from the source SGSN to the target MME over the S3 interface as part of inter-RAT handover and combined hard handover and SRNS relocation procedures, or from the source SGSN to the target SGSN over the S16 interface as part of the SRNS relocation and PS handover procedures.

The new MME/SGSN should send the context request message to the old MME/SGSN on the S3/S16/S10 interface as part of the TAU/RAU procedure to get the MM and EPS bearer contexts for the UE. If the UE identifies itself with a temporary identity and it has changed SGSN/MME since detaching in the attach procedure, the new MME/SGSN should send an identification request message to the old SGSN/MME over the S3, S16, or S10 interface to request IMSI.

A forward access context notification message should be sent from the old SGSN to the new SGSN over the S16 interface to forward the RNC contexts to the target system, or sent from the old MME to the new MME over the S10 interface to forward the RNC/eNB contexts to the target system.

A detach notification message should be sent from an MME to the associated SGSN, or from an SGSN to the associated MME, as part of the detach procedure if the ISR (Idle Mode Signaling Reduction) is activated between the MME and SGSN for the UE. Possible cause values are:

- "Local Detach."
- "Complete Detach."

"Local Detach" indicates that this detach is local to the MME/SGSN and so the associated SGSN/MME registration where the ISR is activated should not be detached. The MME/SGSN that receives this message including this cause value of "Local Detach" only deactivates the ISR. This cause value should be included in the following procedures:

- MME/SGSN-initiated detach procedure in case of implicit detach.
- HSS-initiated detach procedure.

"Complete Detach" indicates that both the MME registration and the SGSN registration that the ISR is activated for should be detached. This "Complete Detach" cause value should be included in the following procedures:

- UE-initiated detach procedure.
- MME/SGSN-initiated detach procedure in case of explicit detach.

The change notification request message is sent on the S4 interface by the SGSN to the S-GW and on the S5/S8 interface by the S-GW to the PGW as part of location-dependent charging-related procedures.

A relocation cancel request message should be sent from the source MME/SGSN to the target MME/SGSN on the S3/S10/S16 interface as part of the inter-RAT handover cancel procedure and on the S16 interface as part of the SRNS relocation cancel procedure. A relocation cancellation typically happens if:

- a relocation timer expires in the source MME/RNC – this means the relocation/handover cannot be performed within an expected time;
- the UE cannot hand over on the radio interface either because of defects in the UE software (as seen with early releases of HSDPA data cards) or because of the wrong radio interface parameters assigned by the target system (e.g., wrong BCCH ARFCN of the GSM cell).

A configuration transfer tunnel message should be used to tunnel eNB configuration transfer messages from a source MME to a target MME over the S10 interface. The purpose of the eNB direct configuration transfer is to transfer information from an eNB to another eNB in UM. This is a possibility to exchange important information (e.g., UL interference status) between eNBs that are not physically connected using the X2 interface.

The RAN information relay message should be sent on the S3 interface between the SGSN and MME to transfer the RAN information received by an SGSN from BSS or RNS (GERAN Iu mode) or by an MME from eNB.

1.10.12.4 CS Fallback

The purpose of CS fallback is to send service requests for voice calls from LTE/EPC to UMTS/GSM. Network operators running both GSM/UMTS and 4G networks in parallel may optimize their resource

usage by reserving the high-speed PS transmission capabilities of LTE and EPC for PS traffic, while voice calls can be delegated by using CS fallback functions to the reliable and profitable legacy GSM and UMTS network. The following GTP messages support this functionality.

The suspend notification message should be sent on the S11 interface by the MME to the S-GW as part of the CS fallback from E-UTRAN access to UTRAN/GERAN CS domain access-related procedures. It is answered with a suspend acknowledge message by the receiving entity. To suspend the call means to stop the call proceeding for a short time, here as long as is necessary to switch the signaling connection from 4G to UMTS/GSM.

The resume notification message should be sent on the S11 interface by the MME to the S-GW as part of the resume procedure returning from CS fallback to the E-UTRAN. With the resume notification message a previously suspended call is taken back into service. Resume Notification is answered by the receiving entity with Resume Acknowledge.

The CS paging indication should be sent on the S3 interface by the MME to the associated SGSN when ISR is activated as part of mobile-terminated CS services. This will happen if a UE was redirected to UTRAN/GERAN radio access by CS fallback, but paging is still received over the EPS.

1.10.12.5 Non-3GPP-Related Access

The messages for non-3GPP-related access are used to support mobility between E-UTRAN and CDMA2000 radio access networks.

A create forwarding tunnel request message should be sent by a MME to a S-GW as part of the MME configuration resources for indirect data forwarding during the active handover procedure from E-UTRAN to CDMA2000 HRPD access. This message is answered with a create forwarding tunnel response message sent back by the receiving entity.

1.10.12.6 Trace Management

The trace session activation message should be sent on S11 by the MME to the S-GW, and on S5/S8 by the S-GW to the PGW, when session trace is activated for a particular IMSI or IMEI for a UE that is attached and active or attached and idle.

The trace session deactivation message should be sent on S11 by the MME to the S-GW, and on S5/S8 by the S-GW to the PGW, when session trace is deactivated for a particular subscriber that is attached and active or attached and idle.

The report data of the trace functionality has a proprietary structure defined by the individual NEMs.

1.10.13 Transmission Control Protocol (TCP)

Like its sister protocol UDP, TCP is a member of the IP family. However, TCP is a reliable, connection-oriented protocol that has capabilities for error detection, error correction, and in-sequence delivery of data streams. Figure 1.103 shows the generic header format of TCP frames.

As in case of UDP, the source and destination ports identify the application on top of the transport layer. Each TCP packet is sent with a unique sequence number that is acknowledged by the receiver after error-free reception of the packet. There is no separate ACK message. Instead the ACK is transmitted using the next available frame in the opposite direction.

The meaning of the other TCP header information elements is as follows:

- Data offset: The length of the TCP header without the data field (payload).
- Flags (8 bits) (aka control bits): These are eight 1-bit flags with the following meaning:

  - Congestion Window Reduced (CWR) (1 bit): This flag is set by the sending host to indicate that it received a TCP segment with the ECN-Echo (ECE) flag set and had responded in the congestion control mechanism.
  - ECE (1 bit): Value (1) indicates that the TCP peer is ECN capable during three-way handshake, and value (2) that a packet with the congestion experienced flag in the IP header set is received during normal transmission.
  - URG (1 bit): This is the URGent pointer field for datagrams with high priority.
  - ACK (1 bit): This indicates that the ACK field is significant.
  - PSH (1 bit): The push function.
  - RST (1 bit): Reset the connection.
  - SYN (1 bit): Synchronize sequence numbers.
  - FIN (1 bit): No more data from sender. This flag should trigger the TCP FIN procedure to terminate the TCP connection.
- Window (16 bits): This is the size of the receive window, which specifies the number of bytes (beyond the sequence number in the ACK field) that the receiver is currently willing to receive.
- Checksum (16 bits): This 16-bit field is used for error checking of the header *and* the payload data.
- Urgent pointer (16 bits): If the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte.
- Options (variable bits): This is an appendix with optional additional information. The total length of the option field must be a multiple of a 32-bit word and the data offset field adjusted appropriately.

Each TCP connection starts with a so-called three-way handshake, as shown in the first three lines of Figure 1.104.

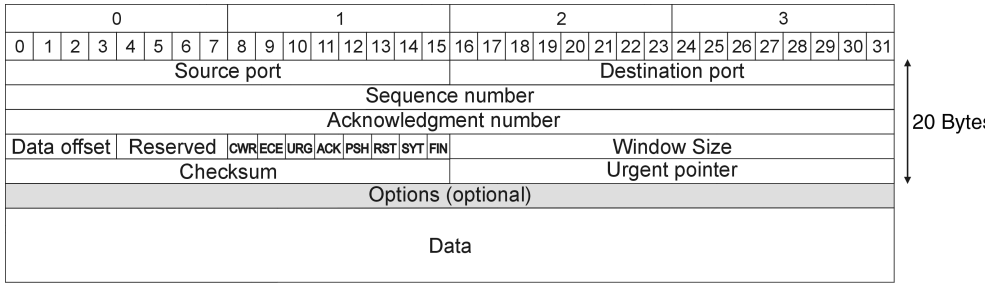


Figure 1.103 TCP header format.

Short View

4. Prot	4. MSG	5. Prot	5. MSG	Source Port	Destination Port	Sequence Number	Acknowledgment Number
TCP	syn			2867 : esps-portal	21 : ftp - File Transfer [Control]	4062981465	0
TCP	syn-ack			21 : ftp - File Transfer [Control]	2867 : esps-portal	1886411453	4062981466
TCP	ack			2867 : esps-portal	21 : ftp - File Transfer [Control]	4062981466	1886411454
TCP	ack	FTP	repl	21 : ftp - File Transfer [Control]	2867 : esps-portal	1886411454	4062981466
TCP	ack	FTP	cmd	2867 : esps-portal	21 : ftp - File Transfer [Control]	4062981466	1886411474
TCP	ack	FTP	repl	21 : ftp - File Transfer [Control]	2867 : esps-portal	1886411474	4062981479
TCP	ack	FTP	cmd	2867 : esps-portal	21 : ftp - File Transfer [Control]	4062981479	1886411508
TCP	ack	FTP	repl	21 : ftp - File Transfer [Control]	2867 : esps-portal	1886411508	4062981495
TCP	ack	FTP	cmd	2867 : esps-portal	21 : ftp - File Transfer [Control]	4062981495	1886411531
TCP	ack	FTP	repl	21 : ftp - File Transfer [Control]	2867 : esps-portal	1886411531	4062981503
TCP	ack	FTP	cmd	2867 : esps-portal	21 : ftp - File Transfer [Control]	4062981503	1886411562
TCP	ack	FTP	repl	21 : ftp - File Transfer [Control]	2867 : esps-portal	1886411562	4062981511
TCP	ack	FTP	cmd	2867 : esps-portal	21 : ftp - File Transfer [Control]	4062981511	1886411582
TCP	ack	FTP	repl	21 : ftp - File Transfer [Control]	2867 : esps-portal	1886411582	4062981519

Figure 1.104 TCP startup for a FTP service.

Firstly, the side that wants to establish a TCP connection sends a TCP SYN message. The sequence number in this SYN message is a random number. The ACK number is always 0, because no received frame needs to be acknowledged.

When the peer entity receives the SYN message it sends back a SYN-ACK including the previous sequence number + 1 as the ACK number. The originating party of the connection will do the same to acknowledge the SYN-ACK with the first payload packet to be sent. Starting with this first payload packet, the size of the payload data field is encoded in the sequence number and the SYN-ACK is again acknowledged with its sequence number value + 1.

Due to the fact that the initial round-trip time must be calculated on each side of the connection, the TCP startup procedure may take quite a while, especially if there is a long distance or a long chain of network nodes between the endpoints. Based on delay measurement results, it has become common to describe this typical behavior as "TCP slow start."

TCP detects missing packets on behalf of timer expiry. The initial timer values on both sides of the connection are calculated during the startup procedure as the initial round-trip time. If the expected ACK for a sent packet does not arrive before the timer in the sending entity expires, the previously sent frame is retransmitted as shown in Figure 1.105.

During the ongoing connection the round-trip time on both endpoints of the connection is adjusted multiple times. However, due to outliers in end-to-end latency, it is also possible that duplicated messages are sent in case the receiving entity detects timeout and hence a necessary retransmission, but the expected frame is indeed received – after the retransmission was already sent.

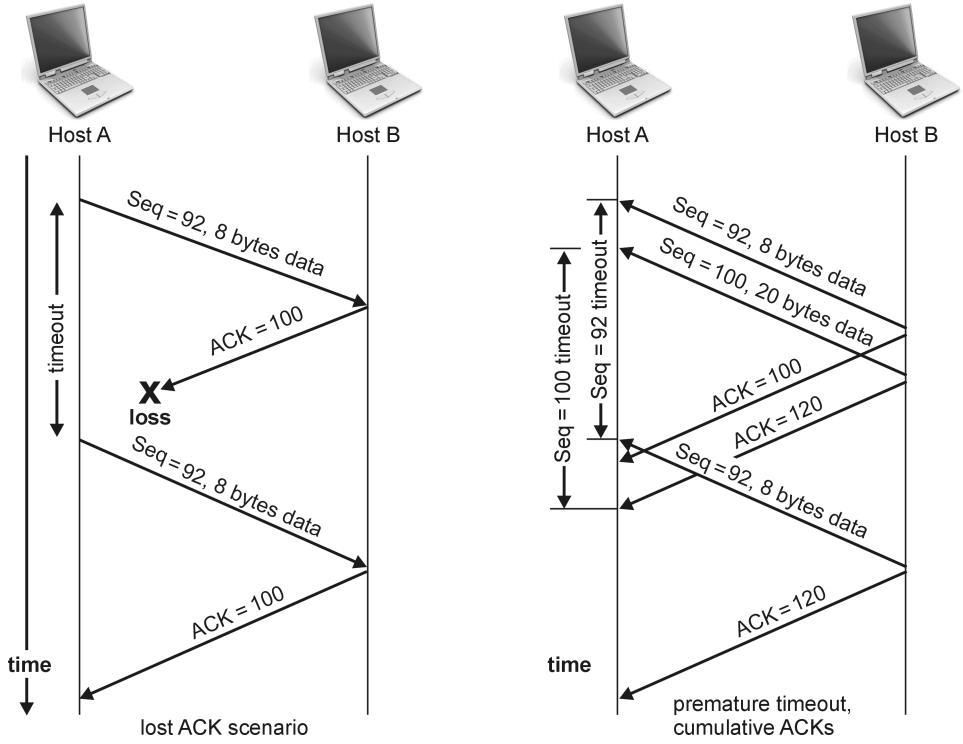


Figure 1.105 TCP retransmission scenarios.

Malfunctions, lost frames, as well as duplicated ACKs have an impact on the network QoS. They slow down the transmission of payload data. Duplicated ACKs are a waste of precious bandwidth on the radio interface and necessary retransmissions increase the payload packet delay.

1.10.14 Session Initiation Protocol (SIP)

SIP is used to establish VoIP calls using the E-UTRAN as the access network. On E-UTRAN interfaces the SIP signaling will run as user plane in-band signaling, which means it can only be monitored inside the user plane bearers.

As all protocols, SIP has its specific terms. In SIP we do not see plain messages, but "methods" that are invoked by clients. Important SIP methods are:

- **REGISTER**: Used to bind a SIP URI address to an IP address.
- **INVITE**: Sent by the originating party to initiate a SIP session. It can be also used to modify an existing session, for instance to add or remove a data stream.
- **BYE**: Used to terminate a session initiated with INVITE.
- **CANCEL**: Used to cancel a pending request, for example, if INVITE was answered with 200OK, but final ACK is missed.
- **OPTIONS**: Can be used by a SIP agent to request a capability list from another SIP agent or from a SIP proxy.
- **MESSAGE**: Used for instant messaging.

In return to a method invoke the receiving SIP party sends back a response code to the originating party. Basically these response codes are identical to the ones used in HTTP/1.1. For a full list, refer to RFC 3261.

The most common response code is 200OK, which is typically sent to acknowledge the reception of a SIP INVITE. Figure 1.106 shows how a SIP session between two users is set up. The terminals in this scenario are called user agents – the term used for a SIP subscriber. The SIP proxies have to make sure that all SIP messages are properly routed. In the architecture of the EPC the SIP proxy functions can be found for example in the IMS.

In step 1 the user agent of Ralf sends an INVITE that contains Karsten's URI. This message is routed through the proxies to Karsten's terminal. As Karsten accepts the session invitation his user

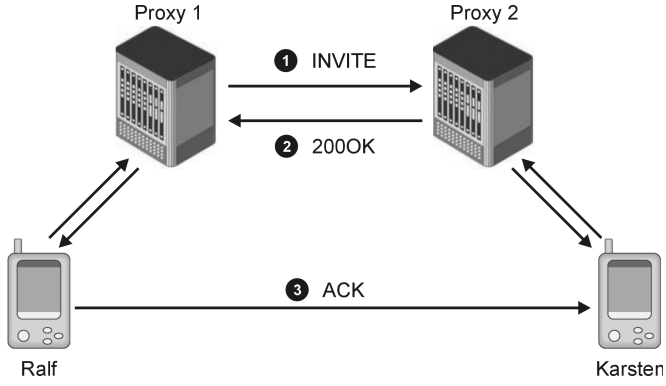


Figure 1.106 SIP session initiation.

agent sends a 200OK response code back to Ralf (step 2). Finally Ralf's user agent sends the final ACK that may be transmitted on a different route not involving the proxies. This is possible because, after the previous messages have been sent, each user agent knows the address of its connection peer.

This SIP call setup procedure is also known as the SIP trapezoid.

SIP by itself does not provide any media format description or QoS indication. For this reason it is generally used in combination with the Session Description Protocol (SDP) that is used to negotiate, for example, the audio codec of the VoIP connection.

1.10.15 DIAMETER on EPC Interfaces

On the EPC network interfaces that are used to connect the HSS with other network elements such as the MME a specific version of the DIAMETER protocol is used. DIAMETER is a protocol designed for authentication, authorization, and accounting. In the IP world it is the successor to the RADIUS protocol. To express the step forward in words, the name DIAMETER was invented as a word play: in geometry the diameter is double the radius. So, in contrast to many other protocols, DIAMETER is not an acronym.

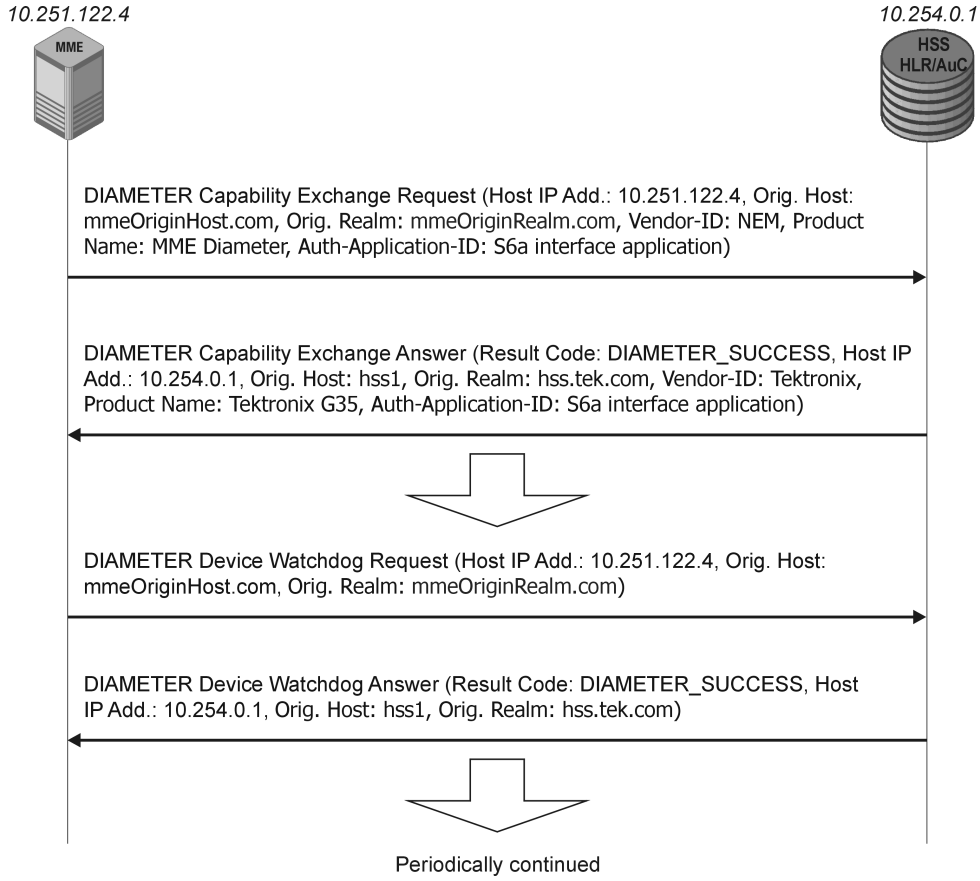


Figure 1.107 MME startup and activity check on S6a reference point.

When looking at EPC DIAMETER decoder output on the S6a interface, there are two groups of messages that can be seen very often: messages for Mobility Service as specified in 3GPP 29.272 and DIAMETER Common Messages according to RFC 3588.

While the mobility service messages will be discussed in the core network call scenarios later in the book, the four most important common messages are shown in the call flow of Figure 1.107. This figure illustrates the message flow that is exchanged between the MME and HSS if a new MME is taken into service.

Whenever a new MME is set up in the network and its DIAMETER protocol entity is starting, this MME will send a DIAMETER Capability Exchange Request to the HSS. The address of the HSS was previously configured in the MME by the network operator. With the capability exchange request message the MME informs the HSS about its IP address as well as its host name and realm name in DNS format. The home realm is an administrative domain. The vendor of the MME is included together with the product name. In these fields we expect very proprietary information. Finally the specific DIAMETER application running on the new network element is indicated: S6a interface applications for Mobility Services.

Message Example 1.2 shows the details of the capability exchange request message. Besides the already mentioned parameters, there is some header information. The hop-by-hop identifier allows tracking of DIAMETER messages on their point-to-point transport connections across the IP transport network, for example, from router to router. The end-to-end identifier allows identification of a DIAMETER message unambiguously by two DIAMETER peer entities. Error bit and retransmission bit have self-explanatory names and underline that DIAMETER is a very reliable protocol.

Message Example 1.2: DIAMETER Capabilities Exchange Request

```
|DIAMETER CER (= Capabilities-Exchange-Request (RFC3588))                    |
|1 Capabilities-Exchange-Request (RFC3588)                                   |
|Diameter Version                    |1                                      |
|Message Length                      |180                                    |
|Request-Bit                         |The message is a request               |
|Proxiable-Bit                       |Message MUST be locally processed      |
|Error-Bit                           |Message contains no error              |
|T(re-transmission)-Bit              |No re-transmission indication          |
|Spare                               |'0000'B                                |
|Command Code                        |Capabilities-Exchange-Request          |
|Application-ID                      |Diameter Common Messages               |
|Hop-by-Hop Identifier               |'653740ce'H                            |
|End-to-End Identifier               |'3e927b1f'H                            |
|1.1 Diameter AVPs                                                           |
|1.1.1 Host-IP-Address                                                       |
|1.1.1.1 Host-IP-Address (RFC 3588)                                          |
|AVP Code                            |Host-IP-Address                        |

|1.1.1.1.1.1 Address                                                        |
|Address-Type                        |IP (IP version 4)                      |
|Address                             |10.251.122.4                           |
|1.1.2 Origin-Host                                                           |
|1.1.2.1 Origin-Host (RFC 3588)                                              |
|AVP Code                            |Origin-Host                            |

|Origin-Host                         |"mmeOriginHost.com"                    |
|1.1.3 Origin-Realm                                                          |
|1.1.3.1 Origin-Realm (RFC 3588)                                             |
|AVP Code                            |Origin-Realm                           |

|Origin-Realm                        |"mmeOriginRealm.com"                   |
|1.1.4 Vendor-Id                                                             |

|Vendor-Id                           |NEM                                    |
```

```
|1.1.5 Product-Name                                                    |
|1.1.5.1 Product-Name (RFC 3588)                                       |

|Product-Name                          |"MME Diameter"                 |
|1.1.6 Auth-Application-Id                                             |
|1.1.6.1 Auth-Application-Id (RFC 3588)                                |

|Auth-Application-Id                   |S6a interface application      |
|1.1.8 Vendor-Specific-Application-Id                                  |
|1.1.8.1 Vendor-Specific-Application-Id (RFC 3588)                     |

|Auth-Application-Id                   |S6a interface application      |
|1.1.8.1.1.2 Vendor-Id                                                 |
|1.1.8.1.1.2.1 Vendor-Id (RFC 3588)                                    |

|Vendor-Id                             |3GPP                           |
```

In response to the capability exchange request message the HSS will send a capability exchange answer message, as shown in Message Example 1.3. This message contains the IP address, host name and realm name of the HSS, and the DIAMETER Result Code. The Result Code indicates a successful procedure on the HSS side or, in the case of failure, it contains the appropriate error cause.

Message Example 1.3: DIAMETER Capabilities Exchange Answer

```
|DIAMETER CEA (= Capabilities-Exchange-Answer (RFC3588)                |
|1 Capabilities-Exchange-Answer (RFC3588)                              |
|Diameter Version                      |1                              |
|Message Length                        |160                            |
|Request-Bit                           |The message is an answer       |
|Proxiable-Bit                         |Message MUST be locally processed|
|Error-Bit                             |Message contains no error      |
|T(re-transmission)-Bit                |No re-transmission indication  |
|Command Code                          |Capabilities-Exchange-Answer   |
|Application-ID                        |Diameter Common Messages       |
|Hop-by-Hop Identifier                 |'653740ce'H                    |
|End-to-End Identifier                 |'3e927b1f'H                    |
|1.1 Diameter AVPs                                                     |
|1.1.1 Result-Code                                                     |
|1.1.1.1 Result-Code (RFC 3588)                                        |
|AVP Code                              |Result-Code                    |

|Result-Code                           |DIAMETER_SUCCESS               |
|1.1.2 Origin-Host                                                     |
|1.1.2.1 Origin-Host (RFC 3588)                                        |

|Origin-Host                           |"hss1"                         |
|1.1.3 Origin-Realm                                                    |
|1.1.3.1 Origin-Realm (RFC 3588)                                       |

|Origin-Realm                          |"hss.tek.com"                  |
|Padding                               |'00'H                          |
|1.1.4 Host-IP-Address                                                 |
|1.1.4.1 Host-IP-Address (RFC 3588)                                    |
|AVP Code                              |Host-IP-Address                |

|Address-Type                          |IP (IP version 4)              |
|Address                               |10.254.0.1                     |
|1.1.5 Vendor-Id                                                       |
|1.1.5.1 Vendor-Id (RFC 3588)                                          |

|Vendor-Id                             |Tektronix Communications       |
|1.1.6 Product-Name                                                    |
|1.1.6.1 Product-Name (RFC 3588)                                       |
```

```
|Product-Name                          |"Tektronix G35"                          |
|1.1.7 Vendor-Specific-Application-Id                                          |
|1.1.7.1 Vendor-Specific-Application-Id (RFC 3588)                             |

|Vendor-Id                             |3GPP                                     |
|1.1.7.1.1.2 Auth-Application-Id                                               |

|Auth-Application-Id                   |S6a interface application                |
```

Now, after the two peer entities have exchanged their address information and capabilities they will check the availability of their connection periodically using a heartbeat check procedure. The DIAMETER-specific name for this period check is the device watchdog procedure and it works as follows.

One entity sends a DIAMETER device watchdog request message (as shown in Message Example 1.4) containing the host name and real name of the sender.

Message Example 1.4: DIAMETER Device Watchdog Request

```
|DIAMETER DWR (= Device-Watchdog-Request (RFC3588))                            |
|1 Device-Watchdog-Request (RFC3588)                                           |

|Command Code                          |Device-Watchdog-Request                  |
|Application-ID                        |Diameter Common Messages                 |
|Hop-by-Hop Identifier                 |'653740d0'H                              |
|End-to-End Identifier                 |'3f3db3e6'H                              |
|1.1 Diameter AVPs                                                             |
|1.1.1 Origin-Host                                                             |
|1.1.1.1 Origin-Host (RFC 3588)                                                |
|AVP Code                              |Origin-Host                              |

|Origin-Host                           |"mmeOriginHost.com"                      |
|Padding                               |'000000'H                                |
|1.1.2 Origin-Realm                                                            |
|1.1.2.1 Origin-Realm (RFC 3588)                                               |
|AVP Code                              |Origin-Realm                             |

|Origin-Realm                          |"mmeOriginRealm.com"                     |
```

On receiving the Device Watchdog Request the peer entity sends back a Device Watchdog Answer (Message Example 1.5) including the address information and Result Code. Again, the Result Code indicates a successful procedure or, in case of failure, it contains the appropriate error cause.

Message Example 1.5: DIAMETER Device Watchdog Answer

```
|DIAMETER  DWA (= Device-Watchdog-Answer (RFC3588))                            |
|1 Device-Watchdog-Answer (RFC3588)                                            |

|Command Code                          |Device-Watchdog-Answer                   |

|1.1.1.1 Result-Code (RFC 3588)                                                |
|AVP Code                              |Result-Code                              |

|Result-Code                           |DIAMETER_SUCCESS                         |
|1.1.2 Origin-Host                                                             |

|Origin-Host                           |"hss1"                                   |
|1.1.3 Origin-Realm                                                            |
|1.1.3.1 Origin-Realm (RFC 3588)                                               |
|AVP Code                              |Origin-Realm                             |

|Origin-Realm                          |"hss.tek.com"                            |
```

2

E-UTRAN/EPC Signaling

In this second chapter of the book we will take a closer look at the signaling procedures across the wired or fibered transport links of the E-UTRAN (Evolved Universal Terrestrial Radio Access Network) and the EPC (Evolved Packet Core) network. This will give some insight into the details of session and bearer management. Also, it will be explained how the mobile communicates with the network on the Non-Access Stratum (NAS) layer that is responsible for subscriber registration and macro-mobility.

Also in this chapter the signaling procedures on the S1 interface between eNodeB (eNB) and the MME Mobility Management Entity, on S6a between the MME and Home Subscriber Server (HSS), on S11 between the MME and Serving Gateway (S-GW), and on the S5 reference point between S-GW and the packet data network gateway (PDN-GW) will be discussed in detail. This will also provide insight into how the user plane packets are tunneled and routed through the EPC network.

2.1 S1 Setup

The S1 Application Part (S1AP) S1 setup procedure is used to take a new eNB into service. Basically this is the same functionality as the NodeB setup on the Iub interface of 3G Universal Terrestrial Radio Access Network (UTRAN). However, in comparison to the Iub signaling procedure, S1 Setup is simpler. And S1 Setup is directly triggered by the eNB while the 3G NodeB only requests to be audited by the RNC. This means that in the 3G UTRAN the RNC is the master of all NodeB configuration parameters, but in the E-UTRAN the eNB is already configured when it is taken into service, and on behalf of the S1 setup procedure the MME is just informed about the main parameters configured in the eNB that is launched.

2.1.1 S1 Setup: Message Flow

Figure 2.1 shows how the S1 setup procedure is executed for two different eNBs. Each eNB sends an S1AP initiating Message for the S1 setup (Third Generation Partnership Project (3GPP) message name: S1 Setup Request – see Message Example 2.1) to the MME. Each eNB is unambiguously identified by its Global-ENB-ID that consists of the Mobile Country Code (MCC) + Mobile Network Code (MNC) + macroENB-ID. There is also a unique Transaction Area Code (TAC) configured for each eNB in the example. Furthermore, the Source IP address (Scr IP) of the IP transport layer (the IP layer below the Stream Control Transmission Protocol (SCTP)) reveals that each eNB has its own IP address.

With this triplet of configuration parameters (macroENB-ID, TAC, and IP address) the main configuration parameters of these eNBs in the overall E-UTRAN topology have been identified.

LTE Signaling, Troubleshooting and Optimization, First Edition. Ralf Kreher and Karsten Gaenger.
© 2011 John Wiley & Sons, Ltd. Published 2011 by John Wiley & Sons, Ltd.

5. Prot	5. MSG	Procedure Code	tAC	Src IP	Dst IP	macroENB-ID	mME-Group-ID	mME-Code
S1-AP	initiatingMessage	id-S1Setup	'0001'H	10.254.0.3	10.251.122.3	'00001'H		
S1-AP	initiatingMessage	id-S1Setup	'00c8'H	10.254.0.4	10.251.122.3	'0000c'H		
S1-AP	successfulOutcome	id-S1Setup		10.251.122.3	10.254.0.3		'0001'H	'01'H
S1-AP	initiatingMessage	id-Reset		10.254.0.3	10.251.122.3			
S1-AP	successfulOutcome	id-S1Setup		10.251.122.3	10.254.0.4		'0001'H	'01'H
S1-AP	initiatingMessage	id-Reset		10.254.0.4	10.251.122.3			
S1-AP	successfulOutcome	id-Reset		10.251.122.3	10.254.0.3			
S1-AP	successfulOutcome	id-Reset		10.251.122.3	10.254.0.4			

Figure 2.1 Combined S1 setup/reset for two eNodeBs connected to the same MME. (Tektronix Communications).

Message Example 2.1: S1AP S1 Setup Request

```
|S1 Application Protocol TS 36.413 V8.4.0 (2008-12) (S1-AP)  initiatingMessage          |
|s1apPDU                                                                              |
|1 initiatingMessage                                                                  |
|1.1 procedureCode                        |id-S1Setup                                 |
|1.2 criticality                          |reject                                     |
|1.3 value                                                                            |
|1.3.1 protocolIEs                                                                    |
|1.3.1.1 sequence                                                                     |
|1.3.1.1.1 id                             |id-Global-ENB-ID                           |
|1.3.1.1.2 criticality                    |reject                                     |
|1.3.1.1.3 value                                                                      |
|1.3.1.1.3.1 TBCD String                  |'299010'                                   |
|1.3.1.1.3.2 eNB-ID                                                                   |
|1.3.1.1.3.2.1 macroENB-ID                |'0000c'H (12 dec.)                         |
|1.3.1.2 sequence                                                                     |
|1.3.1.2.1 id                             |id-eNBname                                 |
|1.3.1.2.2 criticality                    |ignore                                     |
|1.3.1.2.3 value                          |'0000c0'H (12 dec.)                        |
|1.3.1.3 sequence                                                                     |
|1.3.1.3.1 id                             |id-SupportedTAs                            |
|1.3.1.3.2 criticality                    |reject                                     |
|1.3.1.3.3 value                                                                      |
|1.3.1.3.3.1 supportedTAs-Item                                                        |
|1.3.1.3.3.1.1 tAC                        |'00c8'H (200 dec.)                         |
|1.3.1.3.3.1.2 broadcastPLMNs                                                         |
|1.3.1.3.3.1.2.1 TBCD String              |‘299010‘                                   |
```

Looking at the details of the decoder output shown in Message Example 2.2, it should be mentioned that multiple TACs per eNB are possible; the theoretical maximum number of TACs per eNB based on the size of the TAC information element in the S1AP specification is 256 (8-bit TAC field). Also, the same eNB can serve more than one Public Land Mobile Network (PLMN). The theoretical maximum number of broadcast PLMNs per eNB is six.

In return the MME sends a S1AP successful outcome message for S1 Setup to each eNB using the previously identified IP address and updating the base stations with the Globally Unique MME Identifier (GUMMEI). Figure 2.1 only shows the MME group ID and MME code that are part of the GUMMEI (see Section 1.4.4 of this book).

Message Example 2.2: S1AP S1 Setup Response

```
|S1 Application Protocol TS 36.413 V8.4.0 (2008-12) (S1-AP)  successfulOutcome |
|s1apPDU                                                                      |
|1 successfulOutcome                                                          |
|1.1 procedureCode                          |id-S1Setup                       |
|1.2 criticality                            |reject                           |
|1.3 value                                                                    |
|1.3.1 protocolIEs                                                            |
|1.3.1.1 sequence                                                             |
```

```
|1.3.1.1.1 id                              |id-MMEname                    |
|1.3.1.1.2 criticality                     |ignore                        |
|1.3.1.1.3 value                           |6a 6a 62 48 54 43 67 44       |
|1.3.1.2 sequence                                                         |
|1.3.1.2.1 id                              |id-ServedPLMNs                |
|1.3.1.2.2 criticality                     |ignore                        |
|1.3.1.2.3 value                                                          |
|1.3.1.2.3.1 TBCD String                   |‘299010‘                      |
|1.3.1.3 sequence                                                         |
|1.3.1.3.1 id                              |id-ServedGUMMEIs              |
|1.3.1.3.2 criticality                     |ignore                        |
|1.3.1.3.3 value                                                          |
|1.3.1.3.3.1 gUMMEI                                                       |
|1.3.1.3.3.1.1 TBCD String                 |‘299010‘                      |
|1.3.1.3.3.1.2 mME-Group-ID                |'0001'H                       |
|1.3.1.3.3.1.3 mME-Code                    |'01'H                         |
|1.3.1.4 sequence                                                         |
|1.3.1.4.1 id                              |id-RelativeMMECapacity        |
|1.3.1.4.2 criticality                     |ignore                        |
|1.3.1.4.3 value                           |50                            |
```

In Figure 2.2 the message flow of S1 Setup is shown together with the network topology. The relative MME capacity found in the successful outcome message indicates the relative processing capacity of an MME with respect to the other MMEs in an MME pool. The parameter value ranges from 0 to 255 and is used for balancing the load within an MME pool. It represents the weight factor defined in 3GPP 23.401. A higher weight factor (= higher relative MME capacity) means that this MME is able to handle more User Equipment (UE) connections compared to other MMEs in the same pool. So its load can be increased. If an eNB is connected to multiple MMEs, the MME with the highest weight factor should be selected to set up a new UE connection.

After successful S1 Setup, the S1 connection between the new eNB and the MME is reset using the S1AP reset procedure (not shown in Figure 2.2 but in Figure 2.1). This reset is done to synchronize the S1AP state machines in the peer entities after S1 Setup. Also here the difference from the NodeB setup/audit procedure in 3G UTRAN should be noted: in 3G the audit of a NodeB is triggered by a previous NBAP Reset and new NodeB/cell parameters are assigned by the RNC. In E-UTRAN, S1AP Reset is executed to complete the setup of a new eNB and now parameter changes become effective.

2.1.2 S1 Setup: Failure Analysis

If the MME is not able to perform the S1 setup procedure it will send back an unsuccessful outcome message (S1 Setup Failure) to the eNB as shown in Figure 2.3. This failure message includes a cause value. Typical cause values that can be expected are found in the protocol cause group and miscellaneous cause group of S1 AP:

- Semantic error.
- Abstract syntax error.
- Control processing overload.
- Hardware failure.
- Unspecified.
- Unknown PLMN.

Cause values from the NAS cause group and the radio network layer cause group are not expected to be used in the S1 setup failure message.

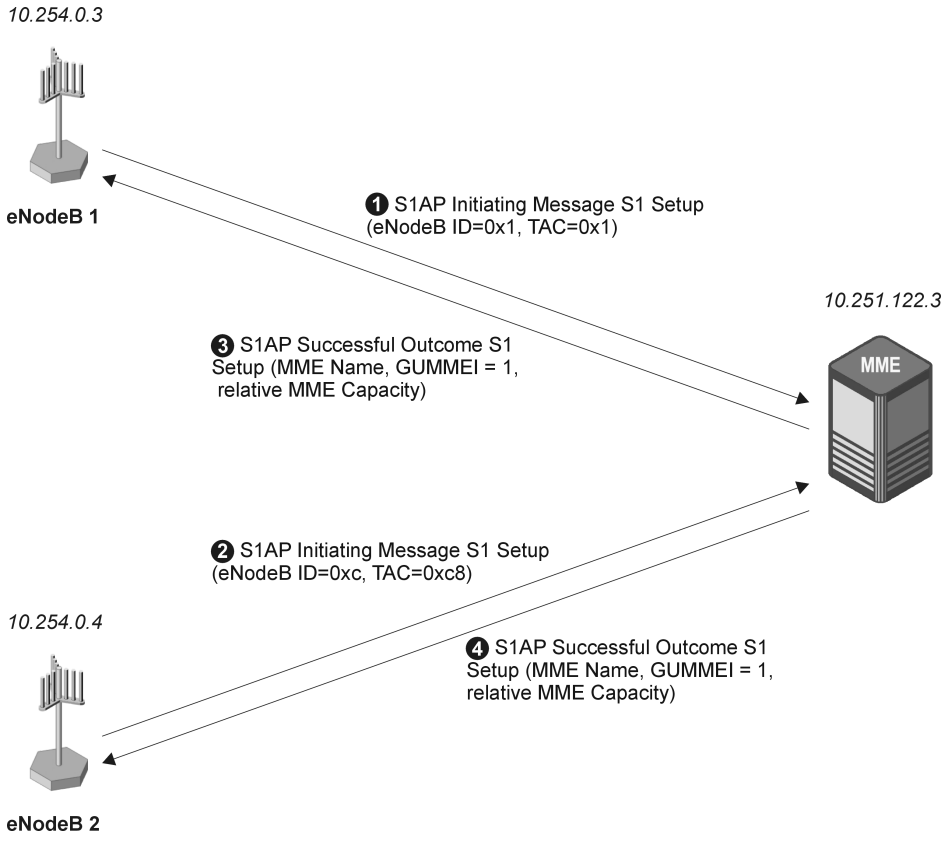


Figure 2.2 S1 Setup for two different eNodeBs. (Tektronix Communications).

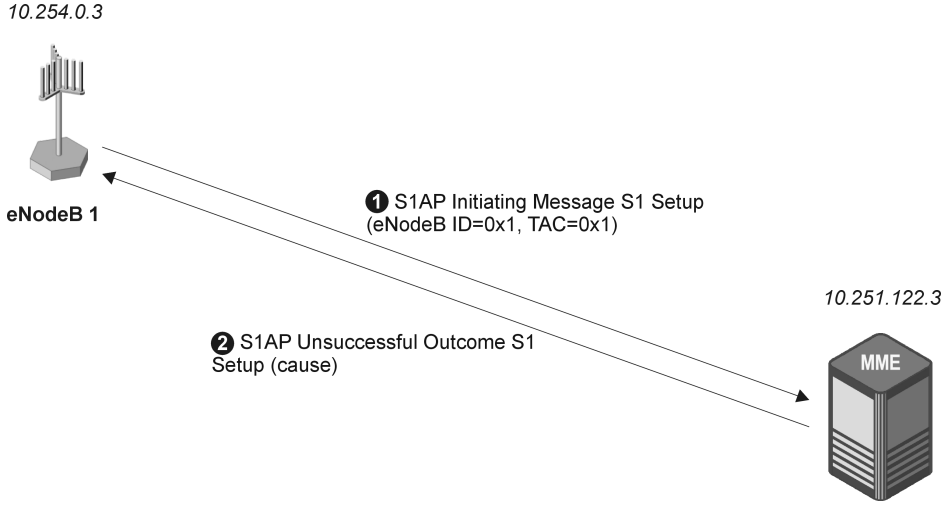


Figure 2.3 S1 Setup failure. (Tektronix Communications).

2.2 Initial Attach

As known from 2G and 3G mobile networks, subscribers need to register to the network. Once the registration is successfully completed, the services offered by the network operator are available for the subscribers.

Typical subscriber actions behind the signaling procedure of attach is to switch on a handset. In the case of data cards or USB sticks commonly used for connecting laptop PCs to the mobile networks, clicking on the CONNECT button of the mobile connection administration software installed together with the device will trigger an attach of the UE.

In addition, as described in 3GPP 23.401, any change in the UE's E-UTRAN capabilities requires the UE to detach and then reattach to the network.

The main difference between an attach to E-UTRAN and one to 3G or 2G RAN is that in E-UTRAN a default bearer for user plane transport will immediately be assigned to the subscriber before the attach is completed. The purpose of this immediate assignment is to reduce the access latency. Indeed, there is not just the S1-U bearer established, but all bearers in the core network on the radio interface that are required to transport payload packets between the UE and the PDN-GW or vice versa. The bearer setup on E-UTRAN and EPC interfaces is embraced by setting up a PDP connection, in core network terminology also called a session. If the subscriber has access to the network, if this access is limited or not, and what kind of service and Quality of Service (QoS) are allowed for this particular subscriber – all these are controlled by the HSS.

As shown in Figure 2.4, the main steps of the attach procedure are as follows.

2.2.1 Procedure

2.2.1.1 Step 1

The mobile sends a NAS attach request message including the type of attach, its permanent or temporary UE identity, and the PDP connection request message. In fact, it is not the UE that communicates on the NAS layer with the MME, but the USIM card. If the USIM card of the UE was never registered to any 4G network before, it will use the International Mobile Subscriber Identity (IMSI) to reveal its identity to the network, otherwise the last Globally Unique Temporary UE Identity (GUTI) stored on the USIM card is used. On S1 the attach request message is transported by the S1AP initial UE message as shown in Message Example 2.3.

Message Example 2.3: S1AP Initial UE Message/NAS Attach Request

ID Name	Comment or Value
S1 Application Protocol TS 36.413 V8.4.0 (2008-12) (including Changes for E-RABToBeSetupItemCtxtSUReq:NAS PDU) (S1-AP) initiatingMessage (= initiatingMessage)	
s1apPDU	
1 initiatingMessage	
1.1 **procedureCode**	id-**initialUEMessage**
1.2 criticality	ignore
1.3 value	
1.3.1 protocolIEs	
1.3.1.1 sequence	
1.3.1.1.1 id	id-**eNB-UE-S1AP-ID**
1.3.1.1.2 criticality	reject
1.3.1.1.3 value	**1**
1.3.1.2 sequence	
1.3.1.2.1 id	id-NAS-PDU
1.3.1.2.2 criticality	reject

```
|1.3.1.2.3 value                        |07 41 01 08 39 01 10 02 10 00 01 10 05 00 00...   |
|1.3.1.3 sequence                                                                          |
|1.3.1.3.1 id                           |id-TAI                                            |
|1.3.1.3.2 criticality                  |reject                                            |
|1.3.1.3.3 value                                                                           |
|1.3.1.3.3.1 TBCD String                |`299000`                                          |
|1.3.1.3.3.2 tAC                        |'00c8'H                                           |
|1.3.1.4 sequence                                                                          |
|1.3.1.4.1 id                           |id-EUTRAN-CGI                                     |
|1.3.1.4.2 criticality                  |ignore                                            |
|1.3.1.4.3 value                                                                           |
|1.3.1.4.3.1 TBCD String                |`299000`                                          |
|1.3.1.4.3.2 cell-ID                    |'0000c00'H                                        |
|NAS LTE TS24.301 V8.0.0 (2008-12) (Secured NAS)  ATRQ (= Attach Request)                  |
|1 Attach Request                                                                          |
|Security header type                   |No security protection                            |
|Protocol discriminator                 |EPS mobility management messages                  |
|Type of Management                     |EPS mobility management                           |
|Message type                           |ATRQ                                              |
|1.1 NAS key set identifier                                                                |
|Type of security context flag (TSC)    |cached security context                           |
|NAS key set identifier                 |0  (Possible values for the NAS key set identi... |
|1.2 EPS attach type                                                                       |
|Spare                                  |0                                                 |
|EPS attach type                        |EPS attach                                        |
|1.3 Old GUTI or IMSI                                                                      |
|Length                                 |8                                                 |
|1.3.1 IMSI                                                                                |
|Type of identity                       |IMSI                                              |
|Odd/Even indicator                     |Odd                                               |
|Identity Digits                        |`299000001001001`                                 |
|1.4 UE network capability                                                                 |
|Length                                 |5                                                 |
|EEA0                                   |EPS encryption algorithm supported                |
|Spare                                  |0                                                 |
|EIA1                                   |EPS integrity algorithm supported                 |
|1xSRVCC                                |SRVCC from E-UTRAN to 3GPP2 1xCS not supported    |
|ISR                                    |The UE does not support ISR                       |
|1.5 ESM Message Container                                                                 |
|Length                                 |32                                                |
|ESM Message Container                  |02 01 d0 11 27 1a 80 21 0a 03 60 00 0a 81 06...   |
|1.6 MS network capability                                                                 |
|Tag                                    |MS network capability                             |
|NAS LTE TS24.301 V8.0.0 (2008-12) (NAS ESM)  PCONRQ (= PDN connectivity request)          |
|1 PDN connectivity request                                                                |
|EPS bearer id                          |0                                                 |
|Protocol discriminator                 |EPS session management messages                   |
|Procedure transaction identity         |1                                                 |
|Type of Management                     |EPS session management                            |
|Message type                           |PCONRQ                                            |
|1.1 PDN type                                                                              |
|Spare                                  |0                                                 |
|PDN type                               |IPv4                                              |
|1.2 Request type                                                                          |
|Spare                                  |0                                                 |
|Request type                           |initial attach                                    |
|1.3 Protocol configuration options                                                        |
|Tag                                    |Protocol configuration options                    |
|Length                                 |26                                                |
|Extension bit                          |1                                                 |
```

```
|Spare                                |'0000'B                                          |
|Configuration protocol               |PPP for use with IP PDP type                     |
|Protocol configuration options       |21 0a 03 60 00 0a 81 06 00 00 00 00 80 21 0a...  |
```

The S1AP initial UE message starts the NAS transport between eNB and the MME. The procedure code information element identifies the message itself. The e-NodeB-UE-S1AP-ID is used during the entire S1AP connection between this eNB and the MME to identify the mobile station unambiguously within the eNB. The first S1AP Downlink (DL) NAS transport message sent by the MME will contain a MME-UE-S1AP-ID value that is the unique identifier of the UE on the S1AP entity of the MME. Both UE-S1AP-IDs form a unique context used to identify the logical S1AP signaling connection for a single UE. Hence, these parameters are key to the design of S1AP call trace functionality.

Together with the NAS PDU (Packet Data Unit – this is the embedded NAS message in raw data format), the eNB sends the current location of the subscriber represented by the tracking area ID and the E-UTRAN Cell Group Identifier (CGI) to the MME. These parameters will later be reported to the HSS during the DIAMETER update location procedure. The TBCD string shown in Message Example 2.3 contains the MCC and MNC of the E-UTRAN. This information is especially important in the case of network sharing, which means the same eNB hardware including antennas can be shared by different network operators.

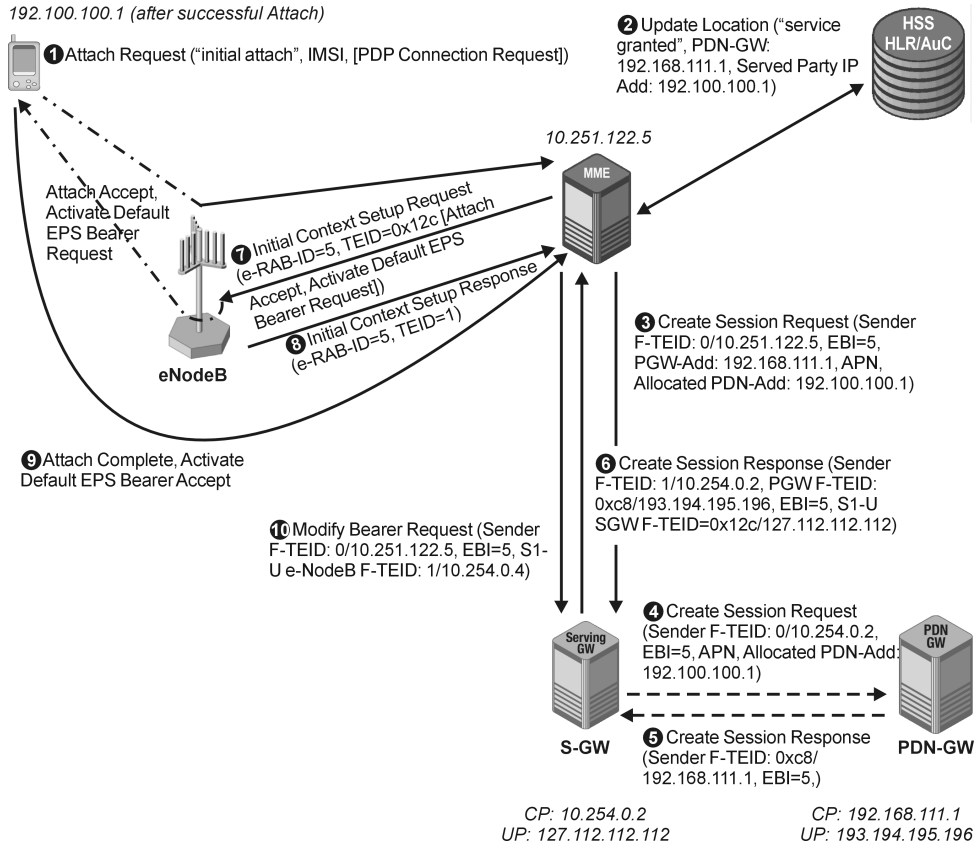


Figure 2.4 E-UTRAN attach procedure. (Tektronix Communications).

When the eNB has received the S-TMSI from the UE during Radio Resource Control (RRC) connection establishment, this parameter will also be included in the S1AP initial UE message.

In Message Example 2.3 the TAC and cell-ID are still decoded in hexadecimal format. Next-generation decoders will translate this into decimal values and performance measurement counters will also use decimal values of these parameters to correlate call-related protocol events such as the attempt counter of the attach procedure with the location of the subscriber.

In the attach request itself, the subscriber's identity can be found. In the case of Message Example 2.3 we see the IMSI here, but attach request messages monitored in live networks will contain the GUTI instead. The security header is a specific information element for the new Long-Term Evolution (LTE) NAS protocol that indicates in Message Example 2.3 that security protection is not yet active for this NAS signaling connection. Indeed, this will be mostly the case for attach request messages, because, typically, activation of security functions is triggered by the network after the initial UE message is received. However, as stated in 3GPP 24.301, an already existing NAS security context does not need to be deleted if the UE detaches from the network. In such a case, if valid NAS security exists on the UE side the attach request message will be integrity protected.

In the attach request message, the Evolved Packet System (EPS) attach type is also found. Possible values for this information element are "EPS attach" and "combined EPS/IMSI attach." "EPS attach" means the UE is allowed to use LTE radio access and the transport services of the EPC network. "IMSI attach" is the protocol term used to describe registration and access to non-EPS services provided by GERAN/UTRAN or other radio access technologies and their appropriate core network transport. A UE that has successfully performed "combined EPS/IMSI attach" can seamlessly be handed over to UTRAN/GERAN, while a UE that has only performed "EPS attach" must remain in E-UTRAN or attach to UTRAN/GERAN before a handover is allowed. It should be noted that a "combined EPS/IMSI attach" may partially fail in such a way that EPS attach is successful, but IMSI attach is not. In such a case, an attach accept message is sent back to the UE and the EPS Mobility Management (EMM) cause value will indicate the reason for the failed IMSI attach.

In the UE network capability section the LTE and UMTS integrity protection and ciphering algorithms supported by the handset that sent the attach request message are indicated. In another section called MS Network Capability, the GERAN-related information is transmitted, for example, the list of supported General Packet Radio Service (GPRS) encryption algorithms.

The PDN connectivity request information is embedded in the ESM message container. As the name of the container already suggests, the PDN Connectivity Request is an EPS session management message while the Attach Request is an EMM message, and these messages are sent in parallel due to the requirement that, in LTE and EPC, for each UE a default bearer needs to be established when the mobile attaches.

The Request Type in the PDN Connectivity Request indicates "initial attach" (as shown in Message Example 2.3) or "handover." In the Protocol Configuration Options typically the dial-in information for the subscriber's Internet access such as user name and password are seen. Addresses of primary and secondary DNS servers can also be found there.

2.2.1.2 Step 2

The Attach Request is received by the MME. This reception triggers the DIAMETER update location procedure on the S6a interface. With this procedure the geographic position of the freshly detected UE is stored in the HSS database and in return the MME receives the subscribed QoS parameters stored in the HSS together with a confirmation that the subscriber is allowed to use the service of the network.

Message Example 2.4 shows an example of the DIAMETER update location request message. The message type is encoded as the DIAMETER Command Code. The Application-ID indicates that this message was monitored on the S6a interface between the MME and HSS. The sender is identified

by Origin Host and Origin Realm, the receiver by its Destination Realm and Destination Host (at the end of the decoded message).

The IMSI of the subscriber who sent the Attach Request is found as "User Name" in the DIAMETER protocol. RAT Type indicates that the E-UTRAN is the radio access technology used by the subscriber and the visited PLMN is identified by the already well-known combination of MCC and MNC.

Message Example 2.4: DIAMETER Update Location Request

ID Name	Comment or Value
DIAMETER based on RFC3588/4005/4006/4072, 3GPP 29.061/.109/.140/.209/.210/.234/.229/.329/32.299 (DIAMETER) ULR (= Update-Location-Request)	
1 **Update-Location-Request**	
Diameter Version	1
Message Length	224
Request-Bit	The message is a request
Proxiable-Bit	Message MAY be proxied, relayed or redirected
Error-Bit	Message contains no error
T(re-transmission)-Bit	No re-transmission indication
Spare	'0000'B
Command Code	**Update-Location-Request**
Application-ID	**S6a interface application**
1.1.3 Origin-Host	
1.1.3.1 Origin-Host (RFC 3588)	
Origin-Host	**"mmeOriginHost.com"**
1.1.4 Origin-Realm	
Origin-Realm	**"mmeOriginRealm.com"**
1.1.5 Destination-Realm	
1.1.5.1 Destination-Realm (RFC 3588)	
Destination-Realm	**"hss.tek.com"**
1.1.6 User-Name	
1.1.6.1 User-Name (RFC 3588)	
User-Name	**"299000001001001"**
1.1.7 RAT-Type	
Vendor-Id	3GPP
RAT-Type	**EUTRAN**
1.1.9 **Visited-PLMN-Id**	
Vendor-Id	3GPP
MCC Digit 1	**2**
MCC Digit 2	**9**
MCC Digit 3	**9**
MNC Digit 3	**0**
MNC Digit 1	**0**
MNC Digit 2	**0**
1.1.10 Destination-Host	
Destination-Host	**"hss1"**

Message Example 2.5 shows the response of the HSS, the DIAMETER update location answer message. It is the Request bit in the DIAMETER header that marks this message as an "Answer" message and again the Application-ID reveals the monitored interface while Origin Real/Host and Destination Realm/Host are the senders/receivers of this message.

The next interesting parameter is the DIAMETER Result Code. This information element distinguishes between a successful and failed update location procedure. In case the value is "Failure," an appropriate cause value will be delivered together with the result code.

The subscriber status information element contains information on whether the desired access to the network is granted to the subscriber or not. Independently of the DIAMETER Result Code, this field may also indicate a failed location update, for example, in the case of roaming subscribers that are not allowed to access the network.

Message Example 2.5: DIAMETER Update Location Answer

ID Name	Comment or Value
DIAMETER based on RFC3588/4005/4006/4072, 3GPP 29.061/.109/.140/.209/.210/.234/.229/.329/32.299 (DIAMETER) ULA (= Update-Location-Answer)	
1 Update-Location-Answer	
Diameter Version	1
Message Length	648
Request-Bit	**The message is an answer**
Proxiable-Bit	Message MAY be proxied, relayed or redirected
Error-Bit	Message contains no error
T(re-transmission)-Bit	No re-transmission indication
Spare	'0000'B
Command Code	Update-Location-Answer
Application-ID	**S6a interface application**
1.1.3.1 Origin-Host (RFC 3588)	
AVP Code	**Origin-Host**
Origin-Host	**"hss1"**
1.1.4 Origin-Realm	
Origin-Realm	**"hss.tek.com"**
1.1.5 Result-Code	
1.1.5.1 Result-Code (RFC 3588)	
AVP Code	Result-Code
Result-Code	**DIAMETER_SUCCESS**
1.1.7.1.1 Subscriber-Status	
Subscriber-Status	**SERVICE_GRANTED**
1.1.7.1.2 AMBR	
1.1.7.1.2.1.1 Max-Requested-Bandwidth-UL	
AVP Code	Max-Requested-Bandwidth-UL
Max-Requested-Bandwidth-UL	**10000000**
1.1.7.1.2.1.2 Max-Requested-Bandwidth-DL	
Max-Requested-Bandwidth-DL	**100000000**
1.1.7.1.3 3GPP-Charging-Characteristics	
1.1.7.1.4 **Access-Restriction-Data**	
HO-To-Non-3GPP-Access Not Allowed	0
E-UTRAN Not Allowed	0
I-HSPA-Evolution Not Allowed	0
GAN Not Allowed	0
GERAN Not Allowed	1
UTRAN Not Allowed	1
1.1.7.1.5 MSISDN	
MSISDN	**`491999792001`**
1.1.7.1.6 **APN-Configuration-Profile**	

```
|Called-Station-Id                    |"rhinophone.com"                                  |
|1.1.7.1.6.1.3.1.3 PDN-Type                                                              |
|AVP Code                             |PDN-Type                                          |

|PDN-Type                             |IPv4                                              |
|1.1.7.1.6.1.3.1.4 VPLMN-Dynamic-Address-Allowed                                         |

|VPLMN-Dynamic-Address-Allowed        |NOT ALLOWED                                       |
|1.1.7.1.6.1.3.1.5 PDN-GW-Identity                                                       |

|1.1.7.1.6.1.3.1.5.1.1.1 PDN-GW-Address                                                  |
|1.1.7.1.6.1.3.1.5.1.1.1.1 Address                                                       |
|Address-Type                         |IP (IP version 4)                                 |
|Address                              |192.168.111.1                                     |
|1.1.7.1.6.1.3.1.5.1.2 PDN-GW-Name                                                       |
|AVP Code                             |PDN-GW-Name                                       |

|PDN-GW-Name                          |"rhinophone.com"                                  |
|1.1.7.1.6.1.3.1.6 PDN-GW-Allocation-Type                                                |

|PDN-GW-Allocation-Type               |STATIC                                            |
|1.1.7.1.6.1.3.1.7 EPS-Subscribed-QoS-Profile                                            |

|1.1.7.1.6.1.3.1.7.1.1 QoS-Class-Identifier                                              |
|AVP Code                             |QoS-Class-Identifier                              |

|QoS-Class-Identifier                 |9                                                 |
|1.1.7.1.6.1.3.1.7.1.2 ARP                                                               |

|1.1.7.1.6.1.3.1.8.1 Served-Party-IP-Address                                             |
|1.1.7.1.6.1.3.1.8.1.1 Address                                                           |
|Address-Type                         |IP (IP version 4)                                 |
|Address                              |192.100.100.1                                     |
|1.1.7.1.6.1.3.1.9 3GPP-Charging-Characteristics                                         |

|1.1.7.1.6.1.3.1.10.1 AMBR AVP-List                                                      |
|1.1.7.1.6.1.3.1.10.1.1 Max-Requested-Bandwidth-UL                                       |

|Max-Requested-Bandwidth-UL           |12000000                                          |
|1.1.7.1.6.1.3.1.10.1.2 Max-Requested-Bandwidth-DL                                       |

|Max-Requested-Bandwidth-DL           |120000000                                         |
```

The Aggregated Maximum Bit Rate (AMBR) for uplink (UL) and DL traffic occurs twice in the message: first related to the subscriber, then related to the Access Point Name (APN). The APN – which is clearly visible in the decoder output – is the PDN gateway itself. The difference between the two AMBR values that are also specified as Maximum Requested Bandwidth is that in the first section where the values 10 Mbps on UL and 100 Mbps on DL have been allocated, this is the maximum bit rate granted to all payload traffic carried by the default bearer. In the second section (below the charging characteristics section) the limits for the aggregated bandwidth of *all bearers* of this single subscriber within the single APN (PDN-GW) are defined. This means that if 10 Mbps is reserved for the default bearer on the UL and 12 Mbps set as Maximum Requested UL Bandwidth for this subscriber on the APN side, then only 2 Mbps is left for other bearers running in parallel with the default bearer.

In general the QoS granted to the subscriber during the update location procedure is defined by the Quality of Service Class Identifier (QCI) that was already described in Chapter 1 of this book. In the message example the QCI has the value 9, which means a non-guaranteed bit rate handled with best effort by the network.

In addition to QoS parameters in the sample call flow and message example, the HSS provides the IP address to this particular UE that will be used as long as it is attached to this network (in the message example: 192.100.100.1). This IP address provided by the HSS is a fixed address stored together with the subscriber's QoS according to the service level agreement in its HSS. However, the

most common scenario of IP address allocation that is expected to be seen later in live networks is the assignment of dynamic IP addresses, and the network element responsible for dynamic IP address management and assignment is the PDN-GW.

The HSS also provides the IP address of the PDN-GW together with the APN itself. Having this information, the default route for all IP traffic between this mobile and external IP networks such as the Internet is determined.

2.2.1.3 Step 3

In step 3 this default route needs to be established and the first step is that the MME sends a GPRS Tunneling Protocol (GTP) Create Session Request to the S-GW. This messages reveals the Fully Qualified Tunnel Endpoint Identifier (F-TEID) of the sender that is a combination of a simple Tunnel Endpoint Identifier (TEID) value and the IP address of the MME. Also, the IP address of the UE, its IMSI, the PDN-GW address, and APN (all allocated earlier by the HSS) are included. The EPS Bearer ID (EBI) identifies the particular bearer in case there are more bearers established for the same UE later on.

Message Example 2.6: S11 GTP Create Session Request

ID Name	Comment or Value
Tunnelling Protocol for Control plane (GTPv2-C) 3GPP TS 29.274 V8.0.0 (2008-12) (GTP_C) CSREQ (= Create Session Request)	
1 Create Session Request	
Version	GTPv2
Spare	0
T-Bit	TEID is present in the GTP-C header
Spare	0
Message Type	**Create Session Request**
Message Length	247
TEID	**'00000000'H**
Sequence Number	1
Spare	0
1.1 ieSetCsReq	
1.1.1 **International Mobile Subscriber Identity (IMSI)**	
Type	International Mobile Subscriber Identity (IMSI)
Identity Digits	**'299000001001001'**
1.1.2 RAT Type	
Type	RAT Type
RAT Type	**EUTRAN**
1.1.3 Indication Flags	
Type	Indication
Length	2
CR	1
Spare	0
Instance	0
DAF (Dual Address Bearer)	0
DTF (Direct Tunnel)	0
HI (Handover Indication)	0
DFI (Direct Forwarding Indication)	0
OI (Operation Indication)	0
ISRSI (Idle Mode Signalling Reduction..	0
ISRAI (Idle Mode Signalling Reduction..	0
SGWCI (SGW Change Indication)	0
Spare	0
PT (Protocol Type)	1
TDI (Teardown Indication)	0

```
|SI (Scope Indication)                  |0                                          |
|MSV (MS Validated)                     |0                                          |
|1.1.4 Sender F-TEID for Control Plane  |                                           |
|Type                                   |Fully Qualified Tunnel Endpoint Identifier (F-...|

|Interface Type                         |S11 MME GTP-C interface                    |
|TEID/GRE Key                           |'00000000'H                                |
|IPv4 Address                           |10.251.122.5                               |
|Spare                                  |0                                          |
|EPS Bearer ID (EBI)                    |5                                          |
|1.1.5 PDN Type                         |                                           |
|Type                                   |PDN Type                                   |

|PDN type                               |IPv4                                       |
|1.1.6 Maximum APN Restriction          |                                           |
|Type                                   |APN Restriction                            |
|Restriction Type                       |No Existing Contexts or Restrictions       |
|1.1.7 Bearer Context to be created     |                                           |
|Type                                   |Bearer Context                             |
|1.1.7.1 Information Elements           |                                           |
|1.1.7.1.1 EPS Bearer ID (EBI)          |                                           |
|Type                                   |EPS Bearer ID (EBI)                        |
|EPS Bearer ID (EBI)                    |5                                          |
|1.1.7.1.2 Bearer Level Quality of Service (Bearer QoS)|                                   |
|Type                                   |Bearer Level Quality of Service (Bearer QoS)|

|ARP                                    |3                                          |
|QCI                                    |Network selects the QCI 9 [UL]             |
|Maximum bit rate for uplink            |00 00 00 00 00                             |
|Maximum bit rate for downlink          |00 00 00 00 00                             |
|Guaranteed bit rate for uplink         |00 00 00 00 00                             |
|Guaranteed bit rate for downlink       |00 00 00 00 00                             |
|1.1.8 MSISDN                           |                                           |
|Type                                   |MSISDN                                     |
|MSISDN                                 |‘491999792001‘                             |
|1.1.9 User Location Info (ULI)         |                                           |
|Type                                   |User Location Info (ULI)                   |
|E-UTRAN Cell Global Identification (E..|is included                                |
|Tracking Area Identity (TAI)           |is included                                |
|Routing Area Identification (RAI)      |is not included                            |
|Service Area Identity (SAI)            |is not included                            |
|Cell Global Identification (CGI)       |is not included                            |
|1.1.9.1 TAI Contents                   |                                           |
|MCC                                    |‘299‘                                      |
|MNC                                    |‘000‘                                      |
|TAC                                    |'00c8'H                                    |
|1.1.9.2 ECGI Contents                  |                                           |
|MCC                                    |‘299‘                                      |
|MNC                                    |‘000‘                                      |
|Spare                                  |0                                          |
|ECI                                    |'00c0000'H                                 |
|1.1.10 Serving Network                 |                                           |
|Type                                   |Serving Network                            |
|MCC                                    |‘299‘                                      |
|MNC                                    |‘000‘                                      |
|1.1.11 PGW S5/S8 Address for Control Plane or PMIP|                                   |
|Type                                   |Fully Qualified Tunnel Endpoint Identifier (F-...|
|Length                                 |9                                          |
|CR                                     |1                                          |
|Spare                                  |0                                          |
|Instance                               |1                                          |
|IPv4 Address                           |is included                                |
```

```
|IPv6 Address                          |is not included                          |
|EPS Bearer Id                         |is not included                          |
|Interface Type                        |S5/S8 PGW PMIPv6 interface               |
|TEID/GRE Key                          |'00000000'H                              |
|IPv4 Address                          |192.168.111.1                            |
|1.1.12 Access Point Name (APN)                                                  |
|Type                                  |Access Point Name (APN)                  |
|1.1.12.1 Access Point Name                                                      |
|Length Of Label                       |49                                       |
|Accesspoint name label                |"rhinophone.com"                         |

|1.1.14 PDN Address Allocation (PAA)                                             |
|Type                                  |PDN Address Allocation (PAA)             |

|PDN type                              |IPv4                                     |
|PDN address (IPv4)                    |192.100.100.1                            |
|1.1.15 Aggregate Maximum Bit Rate (AMBR)                                        |
|Type                                  |Aggregate Maximum Bit Rate (AMBR)        |
|APN-AMBR for uplink [kbps]            |12000000                                 |
|APN-AMBR for downlink [kbps]          |120000000                                |
|1.1.16 Protocol Configuration Options (PCO)                                     |
|Type                                  |Protocol Configuration Options (PCO)     |
```

A look at Message Example 2.6 shows the detailed contents and structure of the GTP create session request message. It is quite interesting, because it reveals many different addresses. There are the IMSI and MSISDN of the subscriber, the IP address of the PDN-GW/APN, the IP address assigned to the subscriber, and the IP address of the MME. There are the EBIs (= 5) together with the previously discussed QCI and the maximum and guaranteed bit rate values (they are all set to zero, because QCI value "9" indicates "best effort"). Also Tracking Area Identity (TAI) and E-UTRAN Cell Group Identifier (ECGI) are included and allow the determination of the current location of the subscriber. Finally, the protocol configuration options (e.g., user name and password of the Internet service provider) are also included.

In the RAT Type there are furthermore a couple of flags that signal if the UE supports functions like idle mode signaling reduction, a mechanism to limit signaling during inter-RAT cell reselection in idle mode. It is also indicated if the create session request message is sent as part of the handover or data forwarding procedure.

2.2.1.4 Step 4

The Create Session Request received by the S-GW triggers another create session procedure, this time between S-GW and PDN-GW. Again the IP addresses of the involved network elements and the EBI can be found in the GTP signaling messages. The arrows of these messages in Figure 2.4 are dashed, because the S5 interface was not monitored in the real-world scenario discussed in this chapter. The PDN-GW also receives the IP address of the UE and the APN value.

2.2.1.5 Step 5

With the GTP create session response message the PDN-GW confirms reception of all UE-related information and completes the setup of the S5 bearer.

2.2.1.6 Step 6

Now the S-GW signals completion of the session and bearer setup to the MME across the S11 interface. Since the payload on the way from the UE to the S-GW will be routed on a different interface (S1-U), a special F-TEID for the S1-U user plane entity of the S-GW is signaled to the

MME. Also, the routing information for the PDN-GW is sent to the MME. This gives the MME full control of all user plane packet routing and it is later up to the MME to select new routes due to the mobility of subscribers or due to changing load conditions in the packet core entities.

2.2.1.7 Step 7

After the bearers in the core network have been established, it is now necessary to establish user plane transport functions on the radio interface as well as on S1. A S1AP initial context setup request message is sent by the MME to the eNB. It includes all UE-specific parameters to be stored in the eNB, the user plane TEID of the S-GW for GTP tunnel establishment on S1-U, and the NAS messages Attach Accept and Activate Default Bearer Request that are transparently forwarded to the UE over the radio interface. An example of this important, but very complex signaling message is given in Message Example 2.7 (where all transport layer and redundant decoder outputs have been deleted to highlight the essential parts).

Message Example 2.7: S1AP Initial Context Setup Request/NAS Attach Accept/Activate Default Bearer Request

```
+--------------------------------------+-------------------------------------------------+
|ID Name                               |Comment or Value                                 |
+--------------------------------------+-------------------------------------------------+
|S1 Application Protocol TS 36.413 V8.4.0 (2008-12) (including Changes for E-
RABToBeSetupItemCtxtSUReq:NAS PDU) (S1-AP)  initiatingMessage (= initiatingMessage)      |
|s1apPDU                                                                                 |
|1 initiatingMessage                                                                     |
|1.1 procedureCode                     |id-InitialContextSetup                           |
|1.2 criticality                       |reject                                           |
|1.3 value                                                                               |
|1.3.1 protocolIEs                                                                       |
|1.3.1.1 sequence                                                                        |
|1.3.1.1.1 id                          |id-MME-UE-S1AP-ID                                |
|1.3.1.1.2 criticality                 |reject                                           |
|1.3.1.1.3 value                       |0                                                |
|1.3.1.2 sequence                                                                        |
|1.3.1.2.1 id                          |id-eNB-UE-S1AP-ID                                |
|1.3.1.2.2 criticality                 |reject                                           |
|1.3.1.2.3 value                       |1                                                |
|1.3.1.3 sequence                                                                        |
|1.3.1.3.1 id                          |id-uEaggregateMaximumBitrate                     |
|1.3.1.3.2 criticality                 |reject                                           |
|1.3.1.3.3 value                                                                         |
|1.3.1.3.3.1 uEaggregateMaximumBitRateDL|'05f5e100'H                                      |
|1.3.1.3.3.2 uEaggregateMaximumBitRateUL|'989680'H                                        |
|1.3.1.4 sequence                                                                        |
|1.3.1.4.1 id                          |id-E-RABToBeSetupListCtxtSUReq                   |
|1.3.1.4.2 criticality                 |reject                                           |
|1.3.1.4.3 value                                                                         |
|1.3.1.4.3.1 sequenceOf                                                                  |
|1.3.1.4.3.1.1 id                      |id-E-RABToBeSetupItemCtxtSUReq                   |
|1.3.1.4.3.1.2 criticality             |reject                                           |
|1.3.1.4.3.1.3 value                                                                     |
|1.3.1.4.3.1.3.1 e-RAB-ID              |5                                                |
|1.3.1.4.3.1.3.2 e-RABlevelQoSParameters                                                 |
|1.3.1.4.3.1.3.2.1 qCI                 |9                                                |
|1.3.1.4.3.1.3.2.2 allocationRetentionPriority                                           |
|1.3.1.4.3.1.3.2.2.1 priorityLevel     |spare                                            |
|1.3.1.4.3.1.3.2.2.2 pre-emptionCapabi..|shall-not-trigger-pre-emption                  |
|1.3.1.4.3.1.3.2.2.3 pre-emptionVulner..|not-pre-emptable                               |
```

```
|1.3.1.4.3.1.3.2.3 gbrQosInformation                                                    |
|1.3.1.4.3.1.3.2.3.1 e-RAB-MaximumBitr..| 232 kbps                                      |
|1.3.1.4.3.1.3.2.3.2 e-RAB-MaximumBitr..| 368 kbps                                      |
|1.3.1.4.3.1.3.2.3.3 e-RAB-GuaranteedB..| 504 kbps                                      |
|1.3.1.4.3.1.3.2.3.4 e-RAB-GuaranteedB..| 1088 kbps                                     |
|1.3.1.4.3.1.3.3 transportLayerAddress  |7f 70 70 70 00 00 00 00 00 00 00 00 00 00 00 00  |
|                                       |00 00 00 00                                     |
|1.3.1.4.3.1.3.4 gTP-TEID               |'0000012c'H                                     |
|1.3.1.4.3.1.3.5 nAS-PDU                |27 00 00 00 00 01 07 42 01 54 06 20 13 20 10...  |
|1.3.1.5 sequence                                                                       |
|1.3.1.5.1 id                           |id-UESecurityCapabilities                       |
|1.3.1.5.2 criticality                  |reject                                          |
|1.3.1.5.3 value                                                                        |
|1.3.1.5.3.1 encryptionAlgorithms       |'0000'H                                         |
|1.3.1.5.3.2 integrityProtectionAlgori..|'0000'H                                         |
|1.3.1.6 sequence                                                                       |
|1.3.1.6.1 id                           |id-SecurityKey                                  |

|NAS LTE TS24.301 V8.0.0 (2008-12) (Secured NAS)  IPCMSG (= Integrity protected and
ciphered NAS message)  |
|1 Integrity protected and ciphered NAS message                                         |
|Security header type                   |Integrity protected and ciphered                |
|Protocol discriminator                 |EPS mobility management messages                |
|Message authentication code            |'00000000'H                                     |
|Sequence number                        |1                                               |
|NAS message(s) FFS                     |07 42 01 54 06 20 13 20 10 00 c8 00 5f 52 01...  |
|NAS LTE TS24.301 V8.0.0 (2008-12) (Plain NAS)  ATAC (= Attach Accept)                  |
|1 Attach Accept                                                                        |
|Security header type                   |No security protection                          |
|Protocol discriminator                 |EPS mobility management messages                |
|Type of Management                     |EPS mobility management                         |
|Message type                           |ATAC                                            |
|1.1 Spare Half Octet                                                                   |
|Spare                                  |0                                               |
|1.2 EPS attach result                                                                  |
|Spare                                  |0                                               |
|EPS attach result                      |EPS only                                        |
|1.3 T3412 value                                                                        |
|Timer value unit                       |value is incremented in multiples of decihours  |
|Timer value                            |20                                              |
|1.4 TAI list                                                                           |
|Length                                 |6                                               |
|Spare                                  |0                                               |
|Type of list                           |one PLMN, with consecutive TAC values           |
|Number of elements                     |0                                               |
|1.4.1 Contents                                                                         |
|1.4.1.1 Partial tracking area identity list (001)                                      |
|MCC Digit 1                            |2                                               |
|MCC Digit 2                            |9                                               |
|MCC Digit 3                            |9                                               |
|MNC Digit 3                            |0                                               |
|MNC Digit 1                            |0                                               |
|MNC Digit 2                            |0                                               |
|TAC                                    |200                                             |
|1.5 ESM Message Container                                                              |
|Length                                 |95                                              |
|ESM Message Container                  |52 01 c1 05 09 55 66 77 88 32 31 76 65 72 69...  |
|1.6 GUTI                                                                               |
|Tag                                    |EPS mobile identity                             |
|Length                                 |11                                              |
|1.6.1 GUTI                                                                             |
```

```
|Type of identity                    |GUTI                                          |
|Odd/Even indicator                  |Even                                          |
|Spare                               |15                                            |
|MCC Digit 1                         |2                                             |
|MCC Digit 2                         |9                                             |
|MCC Digit 3                         |9                                             |
|MNC Digit 3                         |0                                             |
|MNC Digit 1                         |0                                             |
|MNC Digit 2                         |0                                             |
|MME Group ID (MMEGI)                |1                                             |
|MME Group Code (MMEC)               |1                                             |
|M-TMSI                              |'c0000000'H                                   |
|1.7 T3402 value                                                                    |
|Tag                                 |GPRS timer                                    |
|Timer value unit                    |value is incremented in multiples of 1 minute |
|Timer value                         |12                                            |
|NAS LTE TS24.301 V8.0.0 (2008-12) (NAS ESM)  ACTDEFRQ (= Activate default EPS bearer
context request)  |
|1 Activate default EPS bearer context request                                      |
|EPS bearer id                       |5                                             |
|Protocol discriminator              |EPS session management messages               |
|Procedure transaction identity      |1                                             |
|Type of Management                  |EPS session management                        |
|Message type                        |ACTDEFRQ                                      |
|1.1 EPS QoS                                                                        |
|Length                              |5                                             |
|QCI                                 |Network selects the QCI 9 [UL]                |
|Maximum bit rate for uplink         |232 kbps                                      |
|Maximum bit rate for downlink       |368 kbps                                      |
|Guaranteed bit rate for uplink      |504 kbps                                      |
|Guaranteed bit rate for downlink    |1088 kbps                                     |
|1.2 Access point name                                                              |
|Length                              |50                                            |
|1.2.1 Access Point Name                                                            |
|Length Of Label                     |49                                            |
|Accesspoint name label              |"rhinophone.com"                              |
|                                    |""                                            |
|1.3 PDN address                                                                    |
|PDN address (IPv4)                  |192.100.100.1                                 |
|1.4 Protocol configuration options                                                 |
|Tag                                 |Protocol configuration options                |
```

Looking closer at the parameters, the eNB-UE-S1AP-ID is the same parameter that was received by the MME in the initial UE message. Now the MME-UE-S1AP-ID is sent back to the eNB to complete the pair of unique context identifiers. All NAS messages of this particular UE connection transported from now on between eNB and the MME or vice versa will have the same ID values.

The UE AMBR values for UL and DL are the same ones that were monitored on the S6a interface (DIAMETER Location Update Response) before. However, in Message Example 2.7 they are still encoded in hexadecimal format.

The next part is the e-RAB-to-be-setup-List. This list contains all information for at least one e-RAB that should be established. If multiple e-RABs are to be established, the list will contain multiple sections of e-RAB-IDs and individual QoS parameters for each Radio Access Bearer (RAB). In the message example there is just one e-RAB to be established. This e-RAB has e-RAB-ID = 5. The value "5" corresponds to the smallest possible NSAPI value used in GPRS Session Management (defined in 3GPP 24.008). The identical value is chosen to ensure the best possible inter-operability between the SGSN and MME.

The transport layer address is a bit string of 32 bits in the case of an IPv4 address and 128 bits in the case of an IPv6 address. In the message example we see an IPv4 address in hexadecimal format

(dotted decimal notation of this string: 127.112.112.112). Thus, all bits reserved for the IPv6 address format are set to "0." The transport layer address identifies the user plane entity of the S-GW. Also, the following GTP TEID belongs to the S-GW side of the user plane tunnel. The UE security capabilities and the security key are sent by the MME to eNB to enable ciphering and integrity protection for the radio interface transmission as described in Section 1.7.

Now comes the NAS part, starting with the attach accept message. This message belongs to EMM as the Protocol Discriminator reveals. The EPS Attach Result shows that an "EPS only" attach was performed – the UE was not registered in the SGSN simultaneously.

The timer T 3412 is used to control periodic Tracking Area Updates. In the message example a value of 20 decihours is signaled to the UE; 1 decihour is 6 minutes. Hence, the UE is requested to perform period tracking area updates every two hours.

The next section of the message contains the Tracking Area List. We see here only one TAC, but indeed the UE can be registered in multiple tracking areas simultaneously.

Finally we see the GUTI, the temporary identity of the UE within the E-UTRAN, and a GPRS timer value of 12 minutes. The purpose of the GPRS timer information element is to specify GPRS specific timer values, for example, for the READY timer that is used to send the UE to the STANDBY state when no data is transmitted during the time of the timer value.

The second NAS message transported by the S1AP Initial Context Setup Request is the Activate Default EPS Bearer Context Request, a session management message sent by the MME to the UE. This message will trigger the setup of a radio bearer on the Uu interface for the defined QoS (Channel Quality Indicator, CQI = 9), the APN, and the UE's IP PDN address assigned earlier by the HSS.

2.2.1.8 Step 8

With the Initial Context Setup Response the eNB confirms the establishment of the GTP tunnel on the S1-U that is part of the RAB. As shown in Message Example 2.8, this message contains an E-RAB-Setup-List in which for each successfully established e-RAB-ID, the user plane transport layer address (here IPv4, dotted decimal notation: 10.254.0.4), and the appropriate GTP TEID of the user plane tunnel endpoint on the eNodeB side are transmitted.

Message Example 2.8: S1AP Initial Context Setup Response

```
|S1 Application Protocol TS 36.413 V8.4.0 (2008-12) (including Changes for E-
RABToBeSetupItemCtxtSUReq:NAS PDU) (S1-AP)  successfulOutcome (= successfulOutcome)       |
|s1apPDU                                                                                  |
|1 successfulOutcome                                                                      |
|1.1 procedureCode                    |id-InitialContextSetup                             |
|1.2 criticality                      |reject                                             |
|1.3 value                                                                                |
|1.3.1 protocolIEs                                                                        |
|1.3.1.1 sequence                                                                         |
|1.3.1.1.1 id                         |id-MME-UE-S1AP-ID                                  |
|1.3.1.1.2 criticality                |ignore                                             |
|1.3.1.1.3 value                      |0                                                  |
|1.3.1.2 sequence                                                                         |
|1.3.1.2.1 id                         |id-eNB-UE-S1AP-ID                                  |
|1.3.1.2.2 criticality                |ignore                                             |
|1.3.1.2.3 value                      |1                                                  |
|1.3.1.3 sequence                                                                         |
|1.3.1.3.1 id                         |id-E-RABSetupListCtxtSURes                         |
|1.3.1.3.2 criticality                |ignore                                             |
|1.3.1.3.3 value                                                                          |
|1.3.1.3.3.1 sequenceOf                                                                   |
|1.3.1.3.3.1.1 id                     |id-E-RABSetupItemCtxtSURes                         |
```

```
|1.3.1.3.3.1.2 criticality             |ignore                                                  |
|1.3.1.3.3.1.3 value                                                                           |
|1.3.1.3.3.1.3.1 e-RAB-ID              |5                                                       |
|1.3.1.3.3.1.3.2 transportLayerAddress |0a fe 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00  |
|                                      |00 00 00 00                                             |
|1.3.1.3.3.1.3.3 gTP-TEID              |'00000001'H                                             |
```

2.2.1.9 Step 9

The UE sends the NAS message Attach Complete in case a new GUTI was assigned with Attach Accept. The assignment of a new GUTI during attach is optional, but is expected to be typically seen in live networks. The other NAS message in this transaction is Activate Default EPS Bearer Accept. With this message the UE confirms that from now on it is ready to send and receive user plane data using the QoS profile assigned to the default bearer.

2.2.1.10 Step 10

After the UE and eNodeB are ready to send/receive payload data, there is only one piece of important information missing to start this data transfer: that is, the S-GW has not yet been informed about the eNodeB's user plane IP address and GTP TEID to be used on S1-U. To close this last open link in the activation chain, a GTP Modify Bearer Request is sent by the MME to the S-GW. This message contains the required information encoded as the S1-U eNodeB F-TEID information element sequence. A GTP modify bearer response message is sent back from the S-GW to the MME (not shown in Figure 2.4).

After this flood of addresses and identifiers, Figure 2.5 shows a summary overview of the involved network elements and identifiers for a particular UE connection and how the signaling and user plane packets are routed through the network.

For the signaling connection between the UE and MME, the UE is now identified by its GUTI. The GUTI is linked to the IMSI that we encountered during the location update procedure on S6a between the MME and HSS, but also on during the create session procedure on S11 between the MME and S-GW and on S5 between S-GW and PDN-GW. These GTP signaling connections for a single UE are now unambiguously marked by the IP addresses of the involved network elements (for S-GW and PDN-GW the IP address for control plane traffic) and on each interface by a pair of TEIDs for the control plane. The same statement is true for the user plane transport tunnels on S1-U and S5. On S5 between S-GW and PDN-GW we can also see how the user plane is separated from the control plane traffic by defining intelligent numbering plans. Indeed, there is no standard document that requires different IP addresses for control plane and user plane traffic in the core network, but from experience gathered in numerous lab and field trial scenarios, it can be postulated that this is a kind of de-facto standard followed by all network equipment manufacturers (NEMs).

The logical connection for one UE on the S1 control plane is embraced by the pair of S1AP-IDs. On the radio interface the same function is provided by the Cell Radio Network Temporary Identifier (C-RNTI) that is signaled on the Medium Access Control (MAC) layer. The C-RNTI is valid for both the user plane and control plane, but eNodeB acts like a switch that sends the control plane traffic across one way to the MME and user plane packets across another way directly to the S-GW.

2.3 UE Context Release Requested by eNodeB

When user inactivity is detected by the network on behalf of timer expiry the default bearer and the UE context between e-NodeB and MME may be deleted at any time when the S1AP UE context release procedure is triggered by eNodeB as illustrated in Figure 2.6.

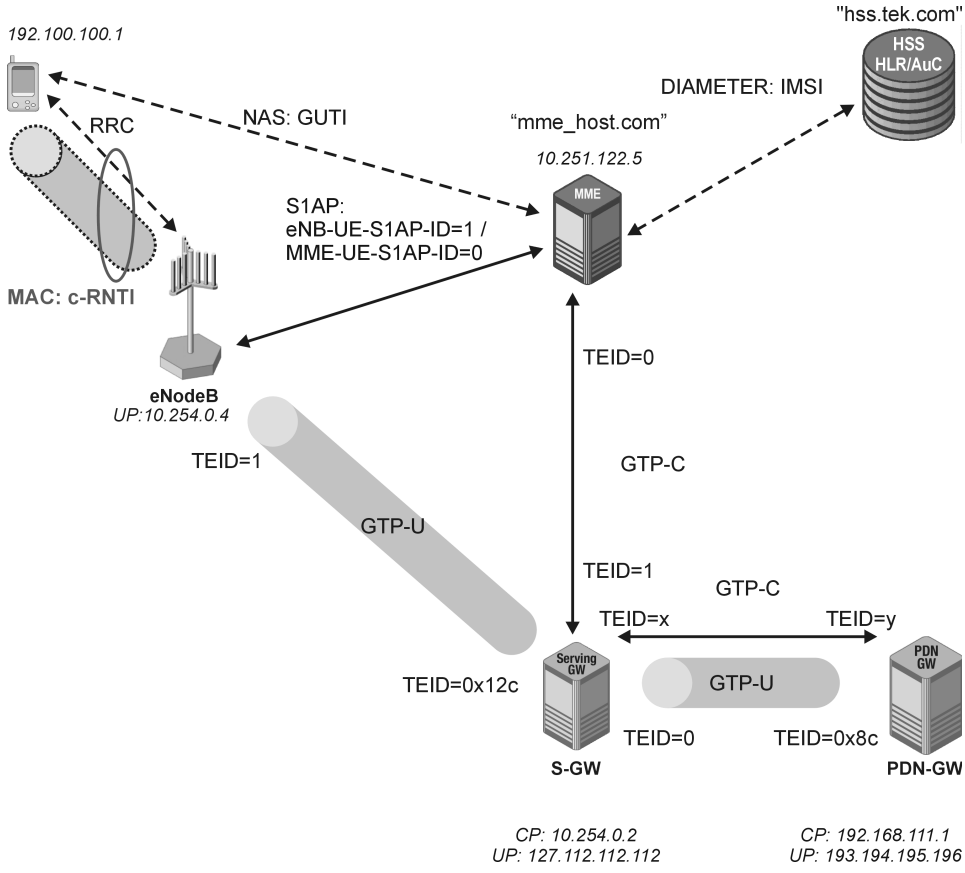


Figure 2.5 Signaling and user plane connection after successful attach. (Tektronix Communications).

Note especially that the UE context release request message is also sent in some other cases, for instance, if the radio connection with the UE is lost and the call drops or if the timer for MME relocation after X2 handover expires.

2.3.1 Procedure

2.3.1.1 Step 1

After the user inactivity timer expires in eNodeB it sends a S1AP UE Context Release Request with the cause value "user inactivity."

2.3.1.2 Step 2

When the MME receives the UE context release request message it triggers release of the S1-U bearer that is executed by sending a GTP modify bearer request message to the S-GW. In this modify bearer request message the Scope Indication flag is set to "1." This is the indication that the associated EPS bearer (in the example identified by EBI = 5) should be deleted and the transport resources related to

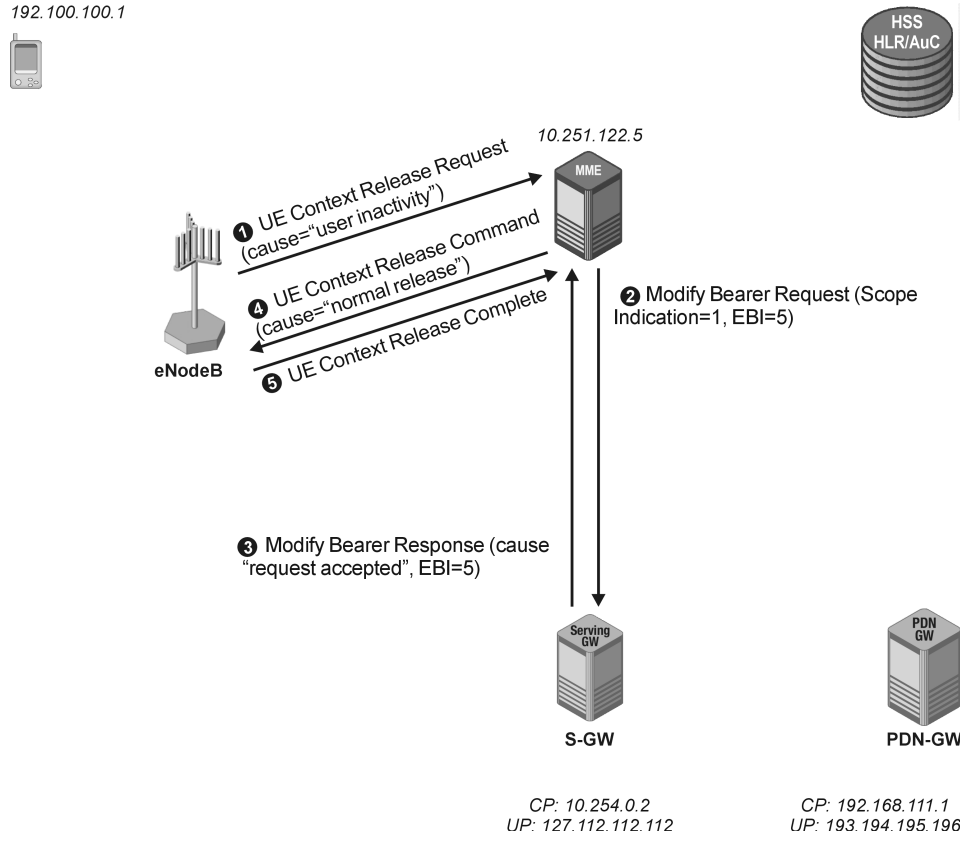


Figure 2.6 UE context release due to user inactivity. (Tektronix Communications).

the bearer, especially the TEID on eNodeB and S-GW side should be released. However, the GTP user plane tunnel between S-GW and PDN-GW remains active and is not deleted during this procedure!

2.3.1.3 Step 3

The S-GW confirms the deletion of the S1-U bearer by sending GTP Modify Bearer Response with the bearer identity (EBI) and the cause "request accepted."

2.3.1.4 Steps 4 and 5

The MME must now also order eNodeB to release the resources for this particular UE connection. This is invoked by sending a S1AP UE context release command to eNodeB. Also, this message contains a cause value. However, since the UE context release command starts the termination of the complete logical S1AP connection, the cause value in this message should not indicate the status of the UE, but rather give an indication if the S1AP connection is normally terminated or not. Hence, this cause message indicates the state of the S1AP state machine in the MME. This state is "normal" even if the connection with the UE on the radio interface has been lost. Unfortunately it cannot be guaranteed that all NEMs have this understanding. In 3G RANAP implementations of different RNC