

Contents

Preface *xiii*

1	Global System for Mobile Communications (GSM)	1
1.1	Circuit-Switched Data Transmission	1
1.1.1	Classic Circuit Switching	2
1.1.2	Virtual Circuit Switching over IP	3
1.2	Standards	4
1.3	Transmission Speeds	5
1.4	The Signaling System Number 7	6
1.4.1	The Classic SS-7 Protocol Stack	7
1.4.2	SS-7 Protocols for GSM	9
1.4.3	IP-Based SS-7 Protocol Stack	10
1.5	The GSM Subsystems	12
1.6	The Network Subsystem	12
1.6.1	The Mobile Switching Center (MSC), Server and Gateway	13
1.6.2	The Visitor Location Register (VLR)	16
1.6.3	The Home Location Register (HLR)	17
1.6.4	The Authentication Center	20
1.6.5	The Short Messaging Service Center (SMSC)	22
1.7	The Base Station Subsystem (BSS) and Voice Processing	24
1.7.1	Frequency Bands	24
1.7.2	The Base Transceiver Station (BTS)	26
1.7.3	The GSM Air Interface	27
1.7.4	The Base Station Controller (BSC)	35
1.7.5	The TRAU for Voice Encoding	39
1.7.6	Channel Coder and Interleaver in the BTS	43
1.7.7	Ciphering in the BTS and Security Aspects	45
1.7.8	Modulation	49
1.7.9	Voice Activity Detection	49
1.8	Mobility Management and Call Control	51
1.8.1	Cell Reselection and Location Area Update	51
1.8.2	The Mobile-Terminated Call	53
1.8.3	Handover Scenarios	56
1.9	The Mobile Device	58
1.9.1	Architecture of a Voice-Centric Mobile Device	58

1.9.2	Architecture of a Smartphone	60
1.10	The SIM Card	62
1.11	The Intelligent Network Subsystem and CAMEL	66
	Questions	69
	References	69

2	General Packet Radio Service (GPRS) and EDGE	71
2.1	Circuit-Switched Data Transmission over GSM	71
2.2	Packet-Switched Data Transmission over GPRS	72
2.3	The GPRS Air Interface	74
2.3.1	GPRS vs. GSM Timeslot Usage on the Air Interface	74
2.3.2	Mixed GSM/GPRS Timeslot Usage in a Base Station	77
2.3.3	Coding Schemes	77
2.3.4	Enhanced Data Rates for GSM Evolution (EDGE)	78
2.3.5	Mobile Device Classes	82
2.3.6	Network Mode of Operation	83
2.3.7	GPRS Logical Channels on the Air Interface	84
2.4	The GPRS State Model	86
2.5	GPRS Network Elements	89
2.5.1	The Packet Control Unit (PCU)	89
2.5.2	The Serving GPRS Support Node (SGSN)	91
2.5.3	The Gateway GPRS Support Node (GGSN)	93
2.6	GPRS Radio Resource Management	94
2.7	GPRS Interfaces	98
2.8	GPRS Mobility Management and Session Management (GMM/SM)	103
2.8.1	Mobility Management Tasks	103
2.8.2	GPRS Session Management	106
	Questions	108
	References	109

3	Universal Mobile Telecommunications System (UMTS) and High-Speed Packet Access (HSPA)	111
3.1	Overview, History and Future	111
3.1.1	3GPP Release 99: The First UMTS Access Network Implementation	113
3.1.2	3GPP Release 4: Enhancements for the Circuit-Switched Core Network	115
3.1.3	3GPP Release 5: High-Speed Downlink Packet Access	116
3.1.4	3GPP Release 6: High-Speed Uplink Packet Access (HSUPA)	117
3.1.5	3GPP Release 7: Even Faster HSPA and Continued Packet Connectivity	117
3.1.6	3GPP Release 8: LTE, Further HSPA Enhancements and Femtocells	118
3.1.7	3GPP Release 9: Digital Dividend and Dual-Cell Improvements	118
3.1.8	3GPP Releases 10 and Beyond	119
3.2	Important New Concepts of UMTS	119
3.2.1	The Radio Access Bearer (RAB)	119
3.2.2	The Access Stratum and Non-Access Stratum	120
3.2.3	Common Transport Protocols for CS and PS	121
3.3	Code Division Multiple Access (CDMA)	121
3.3.1	Spreading Factor, Chip Rate and Process Gain	125

3.3.2	The OVSF Code Tree	126
3.3.3	Scrambling in Uplink and Downlink Direction	127
3.3.4	UMTS Frequency and Cell Planning	128
3.3.5	The Near–Far Effect and Cell Breathing	129
3.3.6	Advantages of the UMTS Radio Network Compared to GSM	131
3.4	UMTS Channel Structure on the Air Interface	132
3.4.1	User Plane and Control Plane	132
3.4.2	Common and Dedicated Channels	132
3.4.3	Logical, Transport and Physical Channels	133
3.4.4	Example: Network Search	137
3.4.5	Example: Initial Network Access Procedure	139
3.4.6	The Uu Protocol Stack	141
3.5	The UMTS Terrestrial Radio Access Network (UTRAN)	146
3.5.1	Node-B, Iub Interface, NBAP and FP	146
3.5.2	The RNC, Iu, Iub and Iur Interfaces, RANAP and RNSAP	147
3.5.3	Adaptive Multirate (AMR) NB and WB Codecs for Voice Calls	152
3.5.4	Radio Resource Control (RRC) States	154
3.6	Core Network Mobility Management	159
3.7	Radio Network Mobility Management	160
3.7.1	Mobility Management in the Cell-DCH State	160
3.7.2	Mobility Management in Idle State	168
3.7.3	Mobility Management in Other States	170
3.8	UMTS CS and PS Call Establishment	172
3.9	UMTS Security	175
3.10	High-Speed Downlink Packet Access (HSDPA) and HSPA+	177
3.10.1	HSDPA Channels	177
3.10.2	Shorter Delay Times and Hybrid ARQ (HARQ)	179
3.10.3	Node-B Scheduling	181
3.10.4	Adaptive Modulation and Coding, Transmission Rates and Multicarrier Operation	182
3.10.5	Establishment and Release of an HSDPA Connection	184
3.10.6	HSDPA Mobility Management	185
3.11	High-Speed Uplink Packet Access (HSUPA)	186
3.11.1	E-DCH Channel Structure	188
3.11.2	The E-DCH Protocol Stack and Functionality	191
3.11.3	E-DCH Scheduling	192
3.11.4	E-DCH Mobility	195
3.11.5	E-DCH-Capable Devices	195
3.12	Radio and Core Network Enhancements: CPC and One Tunnel	196
3.12.1	A New Uplink Control Channel Slot Format	196
3.12.2	CQI Reporting Reduction and DTX and DRX	197
3.12.3	HS-SCCH Discontinuous Reception	198
3.12.4	HS-SCCH-less Operation	198
3.12.5	Enhanced Cell-FACH and Cell/URA-PCH States	199
3.12.6	Radio Network Enhancement: One Tunnel	201
3.13	HSPA Performance in Practice	202
3.13.1	Throughput in Practice	202

3.13.2	Radio Resource State Management	203
3.13.3	Power Consumption	204
3.14	Automated Emergency Calls (eCall) from Vehicles	205
3.15	UMTS and CDMA2000	206
	Questions	207
	References	208

4 Long Term Evolution (LTE) and LTE-Advanced Pro 211

4.1	Introduction and Overview	211
4.2	Network Architecture and Interfaces	214
4.2.1	LTE Mobile Devices and the LTE Uu Interface	215
4.2.2	The eNode-B and the S1 and X2 Interfaces	217
4.2.3	The Mobility Management Entity (MME)	221
4.2.4	The Serving Gateway (S-GW)	222
4.2.5	The PDN-Gateway	223
4.2.6	The Home Subscriber Server (HSS)	224
4.2.7	Billing, Prepaid and Quality of Service	226
4.3	FDD Air Interface and Radio Network	227
4.3.1	OFDMA for Downlink Transmission	227
4.3.2	SC-FDMA for Uplink Transmission	229
4.3.3	Quadrature Amplitude Modulation for Subchannels	231
4.3.4	Reference and Synchronization Signals	233
4.3.5	The LTE Channel Model in the Downlink Direction	234
4.3.6	Downlink Management Channels	235
4.3.7	System Information Messages	236
4.3.8	The LTE Channel Model in the Uplink Direction	237
4.3.9	MIMO Transmission	239
4.3.10	HARQ and Other Retransmission Mechanisms	242
4.3.11	PDPC Compression and Ciphering	245
4.3.12	Protocol Layer Overview	246
4.4	TD-LTE Air Interface	247
4.5	Scheduling	249
4.5.1	Downlink Scheduling	249
4.5.2	Uplink Scheduling	253
4.6	Basic Procedures	253
4.6.1	Cell Search	254
4.6.2	Attach and Default Bearer Activation	256
4.6.3	Handover Scenarios	260
4.6.4	Default and Dedicated Bearers	266
4.7	Mobility Management and Power Optimization	266
4.7.1	Mobility Management in RRC Connected State	266
4.7.2	Mobility Management in RRC Idle State	270
4.7.3	Mobility Management and State Changes in Practice	272
4.8	LTE Security Architecture	273
4.9	Interconnection with UMTS and GSM	274
4.9.1	Cell Reselection between LTE and GSM/UMTS	275
4.9.2	RRC Connection Release with Redirect between LTE and GSM/UMTS	276

4.9.3	Handover from LTE to UMTS	277
4.10	Interworking with CDMA2000 Networks	278
4.10.1	Cell Reselection between LTE and CDMA2000 Networks	279
4.10.2	RRC Connection Release with Redirect between LTE and CDMA2000	279
4.10.3	Handover between LTE and CDMA2000	279
4.11	Carrier Aggregation	280
4.11.1	CA Types, Bandwidth Classes and Band Combinations	281
4.11.2	CA Configuration, Activation and Deactivation	283
4.12	Network Planning Aspects	285
4.12.1	Single Frequency Network	286
4.12.2	Cell-Edge Performance	286
4.12.3	Self-Organizing Network Functionality	287
4.13	CS-Fallback for Voice and SMS Services with LTE	288
4.13.1	SMS over SGs	289
4.13.2	CS-Fallback for Voice Calls	290
4.14	Voice in Combined LTE and CDMA2000 Networks (SV-LTE)	293
4.15	Network Sharing – MOCN and MORAN	293
4.15.1	National Roaming	293
4.15.2	MOCN (Multi-Operator Core Network)	294
4.15.3	MORAN (Mobile Operator Radio Access Network)	295
4.16	From Dipoles to Active Antennas and Gigabit Backhaul	296
4.17	IPv6 in Mobile Networks	298
4.17.1	IPv6 Prefix and Interface Identifiers	298
4.17.2	IPv6 and International Roaming	301
4.17.3	IPv6 and Tethering	301
4.17.4	IPv6-Only Connectivity	303
4.18	Network Function Virtualization	304
4.18.1	Virtualization on the Desktop	304
4.18.2	Running an Operating System in a Virtual Machine	305
4.18.3	Running Several Virtual Machines Simultaneously	306
4.18.4	Virtual Machine Snapshots	306
4.18.5	Cloning a Virtual Machine	307
4.18.6	Virtualization in Data Centers in the Cloud	307
4.18.7	Managing Virtual Machines in the Cloud	308
4.18.8	Network Function Virtualization	308
4.18.9	Virtualizing Routers	310
4.18.10	Software-Defined Networking	310
4.19	Machine Type Communication and the Internet of Things	311
4.19.1	LTE Cat-1 Devices	312
4.19.2	LTE Cat-0 Devices and PSM	313
4.19.3	LTE Cat-M1 Devices	313
4.19.4	LTE NB1 (NB-IoT) Devices	313
4.19.5	NB-IoT – Deployment Options	314
4.19.6	NB-IoT – Air Interface	314
4.19.7	NB-IoT – Control Channels and Scheduling	315
4.19.8	NB-IoT Multicarrier Operation	316
4.19.9	NB-IoT Throughput and Number of Devices per Cell	317

4.19.10	NB-IoT Power Consumption Considerations	317
4.19.11	NB-IoT – High Latency Communication	318
4.19.12	NB-IoT – Optimizing IP-Based and Non-IP-Based Data Transmission	319
4.19.13	NB-IoT Summary	321
4.20	Other Features of LTE-Advanced and LTE-Advanced Pro	321
4.20.1	8 × 8 Downlink and 4 × 4 Uplink MIMO	322
4.20.2	Relays	322
4.20.3	HetNets, ICIC and eICIC	322
4.20.4	Coordinated Multipoint Operation	324
4.21	From LTE to 5G	325
4.21.1	New Radio for 5G	326
4.21.2	Radio Network Evolution for 5G	329
4.21.3	Core Network Evolution for 5G	330
	Questions	330
	References	331

5	VoLTE, VoWifi and Mission Critical Communication	335
5.1	Overview	335
5.2	The Session Initiation Protocol (SIP)	336
5.3	The IP Multimedia Subsystem (IMS) and VoLTE	340
5.3.1	Architecture Overview	340
5.3.2	Registration	342
5.3.3	VoLTE Call Establishment	344
5.3.4	LTE Bearer Configurations for VoLTE	346
5.3.5	Dedicated Bearer Setup with Preconditions	348
5.3.6	Header Compression and DRX	349
5.3.7	Speech Codec and Bandwidth Negotiation	350
5.3.8	Alerting Tone, Ringback Tone and Early Media	353
5.3.9	Port Usage	354
5.3.10	Message Filtering and Asserted Identities	354
5.3.11	DTMF Tones	355
5.3.12	SMS over IMS	356
5.3.13	Call Forwarding Settings and XCAP	357
5.3.14	Single Radio Voice Call Continuity	359
5.3.15	Radio Domain Selection, T-ADS and VoLTE Interworking with GSM and UMTS	362
5.3.16	VoLTE Emergency Calls	364
5.4	VoLTE Roaming	365
5.4.1	Option 1: VoLTE Local Breakout	367
5.4.2	Option 2: VoLTE S8-Home Routing	367
5.5	Voice over WiFi (VoWifi)	369
5.5.1	VoWifi Network Architecture	370
5.5.2	VoWifi Handover	372
5.5.3	Wi-Fi-Preferred vs. Cellular-Preferred	373
5.5.4	SMS, MMS and Supplementary Services over Wi-Fi	373
5.5.5	VoWifi Roaming	374
5.6	VoLTE Compared to Fixed-Line IMS in Practice	375

5.7	Mission Critical Communication (MCC)	376
5.7.1	Overview	376
5.7.2	Advantages of LTE for Mission Critical Communication	377
5.7.3	Challenges of Mission Critical Communication for LTE	378
5.7.4	Network Operation Models	380
5.7.5	Mission Critical Push To Talk (MCPTT) – Overview	381
5.7.6	MCPTT Group Call Establishment	383
5.7.7	MCPTT Floor Control	384
5.7.8	MCPTT Group Call Types	385
5.7.9	MCPTT Configuration and Provisioning	385
5.7.10	eMBMS for MCPTT	386
5.7.11	Priority and Quality of Service	389
	Questions	389
	References	390
6	Wireless Local Area Network (WLAN)	393
6.1	Wireless LAN Overview	393
6.2	Transmission Speeds and Standards	393
6.3	WLAN Configurations: From Ad Hoc to Wireless Bridging	396
6.3.1	Ad Hoc, BSS, ESS and Wireless Bridging	396
6.3.2	SSID and Frequency Selection	399
6.4	Management Operations	400
6.5	The MAC Layer	406
6.5.1	Air Interface Access Control	406
6.5.2	The MAC Header	409
6.6	The Physical Layer and MAC Extensions	410
6.6.1	IEEE 802.11b – 11 Mbit/s	411
6.6.2	IEEE 802.11 g with up to 54 Mbit/s	413
6.6.3	IEEE 802.11a with up to 54 Mbit/s	415
6.6.4	IEEE 802.11n with up to 600 Mbits/s	415
6.6.5	IEEE 802.11 ac – Gigabit Wireless	424
6.6.6	IEEE 802.11ad – Gigabit Wireless at 60 GHz	428
6.7	Wireless LAN Security	432
6.7.1	Wired Equivalent Privacy (WEP)	432
6.7.2	WPA and WPA2 Personal Mode Authentication	434
6.7.3	WPA and WPA2 Enterprise Mode Authentication – EAP-TLS	435
6.7.4	WPA and WPA2 Enterprise Mode Authentication – EAP-TTLS	437
6.7.5	WPA and WPA2 Enterprise Mode Authentication – EAP-PEAP	438
6.7.6	WPA and WPA2 Enterprise Mode Authentication – EAP-SIM	439
6.7.7	WPA and WPA2 Encryption	441
6.7.8	Wi-Fi-Protected Setup (WPS)	442
6.8	IEEE 802.11e and WMM – Quality of Service	444
	Questions	449
	References	450
7	Bluetooth and Bluetooth Low Energy	453
7.1	Overview and Applications	453

7.2	Physical Properties	454
7.3	Piconets and the Master/Slave Concept	457
7.4	The Bluetooth Protocol Stack	459
7.4.1	The Baseband Layer	460
7.4.2	The Link Controller	465
7.4.3	The Link Manager	468
7.4.4	The HCI Interface	469
7.4.5	The L2CAP Layer	470
7.4.6	The Service Discovery Protocol	473
7.4.7	The RFCOMM Layer	474
7.4.8	Overview of Bluetooth Connection Establishment	476
7.5	Bluetooth Security	476
7.5.1	Pairing up to Bluetooth 2.0	477
7.5.2	Pairing with Bluetooth 2.1 and Above (Secure Simple Pairing)	479
7.5.3	Authentication	480
7.5.4	Encryption	481
7.5.5	Authorization	482
7.5.6	Security Modes	483
7.6	Bluetooth Profiles	484
7.6.1	Basic Profiles: GAP, SDP and the Serial Profile	484
7.6.2	Object Exchange Profiles: FTP, Object Push and Synchronize	486
7.6.3	Headset, Hands-Free and SIM Access Profile	489
7.6.4	High-Quality Audio Streaming	492
7.6.5	The Human Interface Device (HID) Profile	495
7.7	Bluetooth Low Energy	495
7.7.1	Introduction	495
7.7.2	The Lower BLE Layers	497
7.7.3	BLE SMP, GAP and Connection Establishment	499
7.7.4	BLE Authentication, Security and Privacy	500
7.7.5	BLE ATT and GATT	501
7.7.6	Practical Example	503
7.7.7	BLE Beacons	504
7.7.8	BLE and IPv6 Internet Connectivity	505
	Questions	507
	References	508

Index	511
--------------	------------