Mobile Networks Architecture

Mobile Networks Architecture

André Pérez

ISTE WILEY

First published 2012 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Cataloging-in-Publication Data

Pérez, André.
Network architecture for mobiles / André Pérez.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-84821-333-3
1. Mobile communication systems--Standards. 2. Cell phone systems--Standards. 3. Computer network architectures. I. Title.
TK5103.2.P447 2012
621.3845'6--dc23

2011045484

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN: 978-1-84821-333-3

Printed and bound in Great Britain by CPI Group (UK) Ltd., Croydon, Surrey CR0 4YY

Table of Contents

Preface ix

Chapter 1. The GSM Network 1

1.1. Services 2
1.2. The architecture of the network 3
1.2.1. Network components. 3
1.2.2. The mobile 4
1.2.3. The radio sub-system. 5
1.2.4. The network sub-system 12
1.3. The radio interface. 17
1.3.1. The transmission chain. 17
1.3.2. Source coding 18
1.3.3. Channel coding 19
1.3.4. Time-division multiplexing 22
1.3.5. Modulation. 34
1.3.6. The frequency plan 34
1.4. Communication management 36
1.4.1. Establishment of the SDCCH. 36
1.4.2. Security management 39
1.4.3. Location management 41
1.4.4. Call management 44
1.4.5. Handover management 47

Chapter 2. The GPRS Network. 53

2.1. Services 54
2.2. Network architecture 56
2.2.1. Network components. 56
2.2.2. Protocol architecture 58

2.2.3. Logical identifiers 61
2.2.4. Mobility context 62
2.2.5. The WAP gateway 64
2.2.6. Roaming between operators. 67
2.3. Radio interface 68
2.3.1. The transmission chain. 68
2.3.2. The MS–BSS interface 69
2.3.3. The MS−SGSN interface 78
2.4. Communication management 85
2.4.1. Roaming management 85
2.4.2. Session management 87
2.4.3. Traffic establishment. 89
2.4.4. Location management 93
2.5. The EDGE evolution 95
2.5.1. The impact on the GSM/GPRS network 95
2.5.2. Modification of the physical layer 96
2.5.3. Modification of the RLC/MAC layer 99
2.5.4. Link control 102

Chapter 3. The UMTS Network 105

3.1. The services 106
3.2. The architecture of the network 107
3.2.1. Network components. 107
3.2.2. Protocol architecture 109
3.2.3. The femtocell 114
3.3. Radio interface 116
3.3.1. The RRC protocol 116
3.3.2. RLC protocol 119
3.3.3. MAC protocol 120
3.3.4. Physical layer 123
3.3.5. The spread spectrum 132
3.3.6. Modulation. 134
3.3.7. The frequency plan 135
3.3.8. Power control 136
3.3.9. The RAKE receiver 137
3.4. Communication management 138
3.4.1. The establishment of a connection for the NAS 138
3.4.2. Paging 139
3.4.3. Establishment of the RAB. 140
3.4.4. Soft handover 141
3.4.5. Relocation 141
3.4.6. Inter-system handover 143

3.5. HSPA evolutions 145
3.5.1. The HSDPA evolution 145
3.5.2. HSUPA evolution. 148
3.5.3. The HSPA+ evolution 151

Chapter 4. The NGN 155

4.1. Network architecture 156
4.1.1. Network components. 156
4.1.2. Protocol architecture 157
4.2. Communication management 164
4.2.1. Communication establishment 164
4.2.2. Communication release 167
4.2.3. The handover 168

Chapter 5. The EPS Network 175

5.1. Network architecture 176
5.1.1. Network components. 176
5.1.2. Protocol architecture 178
5.2. The radio interface. 188
5.2.1. Antenna system 189
5.2.2. Access mode. 190
5.2.3. Frame structure 194
5.2.4. The signals and physical channels 198
5.3. Communication management 211
5.3.1. The attachment procedure 211
5.3.2. Location updating. 214
5.3.3. The establishment of a session 215
5.3.4. Mobility procedure 220

Chapter 6. The IMS Network 227

6.1. The SIP 228
6.1.1. The SIP entities 228
6.1.2. The SIP Identity. 230
6.1.3. The procedures 230
6.2. The IMS architecture 236
6.2.1. Control of sessions 237
6.2.2. The Application Servers 239
6.2.3. The databases 240
6.2.4. The interconnection 240
6.2.5. Multimedia flow processing 241
6.2.6. Charging 241

6.3. Communication management 243
6.3.1. Registration 243
6.3.2. The session. 246

List of Abbreviations 253

Bibliography 263

Index 267

Preface

This work explains the evolutions of architecture for mobiles and summarizes the different technologies:

– 2G: the GSM (Global System for Mobile) network, the GPRS (General Packet Radio Service) network and the EDGE (Enhanced Data for Global Evolution) evolution;

– 3G: the UMTS (Universal Mobile Telecommunications System) network and the HSPA (High Speed Packet Access) evolutions:

- HSDPA (High Speed Downlink Packet Access);

- HSUPA (High Speed Uplink Packet Access);

- HSPA+;

– 4G: the EPS (Evolved Packet System) network.

The telephone service and data transmission are the two main services provided by these networks. The evolutions are fundamentally dictated by the increase in the rate of data transmission across the radio interface between the network and mobiles.

The services are implemented according to two modes:

– the CS (Circuit Service) mode. This mode is characterized by the allocation of a resource dedicated to a flow. This mode provides both types of service;

– the PS (Packet Service) mode. This mode is characterized by the allocation of a resource shared by several flows. This mode is solely used for data transmission.

2G	**Network**	GSM	GPRS	EDGE
	Mode	CS	PS	PS(1)
	Rate	14.4 kbps	171.2 kbps	473.6 kbps(3)

3G	**Network**	UMTS	HSDPA	HSUPA	HSPA+
	Mode	CS and PS	PS	PS	PS
	Rate	64 kbps(2) 384 kbps(3)	14.4 Mbps(4)	5.76 Mbps(5)	43.2 Mbps(4) 11.5 Mbps(5)

4G	**Network**	EPS
	Mode	PS
	Rate	302 Mbps(4) 75 Mbps(5)

(1) The CS mode is rarely used
(2) Rate for the CS mode
(3) Rate for the PS mode
(4) Downlink rate
(5) Uplink rate

Table 1. *Mobile networks – rates*

The network architecture for mobiles reveals two subsystems:

– the AN (Access Network). This sub-system can be used to allocate the radio resource to the mobile, so that it can either be dedicated or shared. It is significantly affected by successive evolutions;

– the CN (Core Network). This sub-system connects the access networks and third-party networks:

- the PSTN (Public Switched Telephone Network);

- the PDN (Packet Data Network);

- the PLMN (Public Land Mobile Network).

The same sub-system is used for the 2G and 3G core networks and consists of two entities:

– the NSS (Network Sub-System) entity provides services in CS mode;

– the GSS (GPRS Sub-System) entity provides services in PS mode.

The 2G and 3G mobile networks mainly differentiate by the type of access network deployed:

– the BSS (Base Station Sub-system) entity for 2G networks;

– the UTRAN (UMTS TRAnsport Network) entity for 3G networks.

The 4G mobile network consists of two entities:

– the access network E-UTRAN (Evolved UTRAN);

– the EPC (Evolved Packet Core) network. It functions in PS mode and solely provides the data transmission service.

2G	**Network**	GSM	GPRS	EDGE
	CN	NSS	GSS	GSS
	AN	BSS	BSS (evolution)	BSS (evolution)

3G	**Network**	UMTS	HSDPA	HSUPA	HSPA+
	CN	NSS and GSS	GSS	GSS	GSS
	AN	UTRAN	UTRAN (evolution)	UTRAN (evolution)	UTRAN (evolution)

4G	**Network**	EPS
	CN	EPC
	AN	E-UTRAN

Table 2. *Mobile networks – architecture*

The NSS entity has evolved into an NGN (Next Generation Network) architecture that is used to separate the functions of telephone traffic transport and signaling processing. Interconnection of the NSS entity machines is ensured by an SDH (Synchronous Digital Hierarchy) transmission network. That of the NGN equipment is implemented by an IP (Internet Protocol) network identical to that deployed for the GSS network.

The 4G network ensures that telephone traffic transport is treated as a source of data. The signaling processing that administers the telephone service is provided by the IMS (IP Multimedia Sub-system), which is an entity external to the mobile network. This IMS entity is independent of the network involved in data transport. It can also be associated with the UMTS network functioning in PS mode.

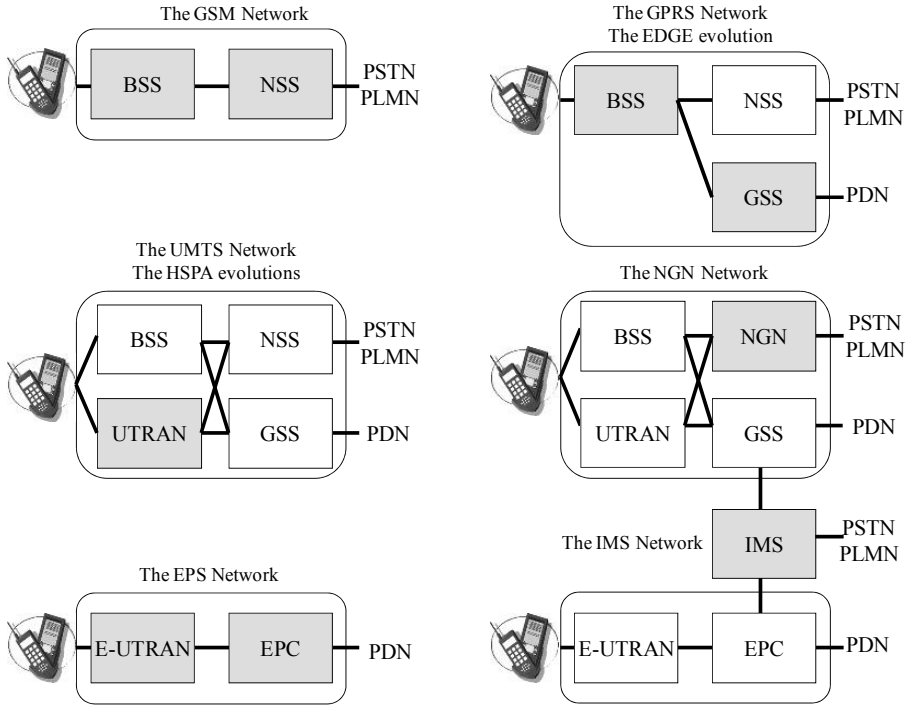


Figure 1. *Mobile networks – the architecture*

The following table summarizes the points covered in the different chapters of this work.

Chapter	**1**	**2**	**3**	**4**	**5**	**6**
Network	GSM	GPRS	UMTS	NGN	EPS	IMS
SIP (Session Initiation Protocol)						✓
Services	✓	✓	✓			
Network architecture	✓	✓	✓	✓	✓	✓
Radio interface	✓	✓	✓		✓	
Communication management	✓	✓	✓	✓	✓	✓
EDGE evolution		✓				
HSPA evolutions			✓			

Table 3. *Mobile networks – the structure of this book*

Chapter 1

The GSM Network

Section 1.1 in this chapter explains the services provided by the GSM (Global System for Mobile) network, the main ones being the telephone service and the data transmission service. These services are implemented in CS (Circuit Service) mode, for which a resource dedicated to a flow is reserved.

Section 1.2 explains the architecture of a GSM network consisting of two sub-systems − the BSS (Base Station Sub-system) access network and the NSS (Network Sub-System) core network − and the MS (Mobile Station).

It also describes the protocol architecture concerning the signaling data enabling the allocation of the resource dedicated to establishment of communications between two mobiles using the same PLMN (Public Land Mobile Network), two mobiles using two different PLMN networks or a mobile and a PSTN (Public Switched Telephone Network) fixed terminal.

Section 1.3 explains the radio interface between the mobile and the mobile network. The description of the transmission channel is essentially concerned with source coding, channel coding, time-division multiplexing of logical channels, modulation and the frequency plan.

Section 1.4 describes the procedures concerning the establishment of an incoming or outgoing call, location (roaming) management and the control of its access to mobile networks.

1.1. Services

The telecommunication services offered by the GSM network are divided into two categories:

– bearer services, which provide the ability to transmit between access points;

– teleservices, which are communication services between users.

Bearer services are used to transfer two types of signal:

– the audio frequency signal (300-3,400 Hz) used for the transfer of speech or data at a rate ≤14.4 kbps;

– the digital UDI (Unrestricted Digital Information) signal at a rate ≤14.4 kbps.

Two modes of digital transmission are defined:

– transparent mode. The network carries out the transfer a bit at a time between the extremities of the mobile network;

– non-transparent mode. The RLP (Radio Link Protocol) is used for the reliable transfer of data.

The data transmission service consists of establishing a circuit between two users or in accessing a data network. The transmission is carried out in synchronous or asynchronous mode.

The telephony teleservice is used for the transmission of speech. The network must also ensure transmission of the following specific signals:

– the tones used in the fixed network;

– the DTMF (Dual-Tone Multi-Frequency) tones in the mobile-to-fixed direction (for example to control voice mail) throughout an established call.

Table 1.1 contains the list of additional services that complement the telephony teleservice.

The VBS (Voice Broadcast Service) allows a user to broadcast a voice message to several other users within a certain geographical area. The user who makes the call is the speaker and the other users are only listeners.

The VGCS (Voice Group Call Service) defines a closed group of users who can speak using a push-to-talk mechanism.

The SMS (Short Message Service) teleservice is used to transmit a text message between a MS and a SMS SC (Service Center). The service center is functionally separated from the GSM network.

The facsimile teleservice is used for Group 3 fax transmission at 9,600 bps using two modes:

– manual mode is used to pass back and forth between speech and fax;

– automatic mode is used to generate or receive a fax call without going via speech.

Type	Abbreviation	Description
Priority call	MLPP	Multi-Level Precedence and Pre-emption service
Number identification	CLIP	Calling Line Identification Presentation
	CLIR	Calling Line Identification Restriction
	COLP	COnnected Line identification Presentation
	COLR	COnnected Line identification Restriction
Call forwarding	CFU	Call Forwarding Unconditional
	CFB	Call Forwarding on mobile subscriber Busy
	CFNRy	Call Forwarding on No Reply
	CFNRc	Call Forwarding on Mobile Not Reachable
Call waiting	CW	Call Waiting
	HOLD	Call is on hold
Call barring	BAOC	Barring of All Outgoing Calls
	BOIC	Barring of Outgoing International Calls
	BOIC − exHC	BOIC except those directed to the Home PLMN (Public Land Mobile Network) Country
	BAIC	Barring of All Incoming Calls

Table 1.1. *List of additional services*

1.2. The architecture of the network

1.2.1. *Network components*

The GSM network consists of two sub-systems (Figure 1.1):

– The BSS radio sub-system: this ensures radio transmission of the mobile, manages the radio resources (RRs) and allows for mobile mobility. The BSS sub-

system consists of BTS (Base Transceiver Station) radio stations, BSC (Base Station Controller) radio station controllers and TRAU (Transcoder/Rate Adaptor Unit) transcoding equipment.

– The NSS is used for call processing in the establishment of communication as well as for roaming and mobility management (MM). The NSS consists of the telephone switches MSC (Mobile-services Switching Center), GMSC (Gateway MSC), TSC (Tandem Switching Center), and the databases HLR (Home Location Register), VLR (Visitor Location Register), AuC (Authentication Center) and EIR (Equipment Identity Register).

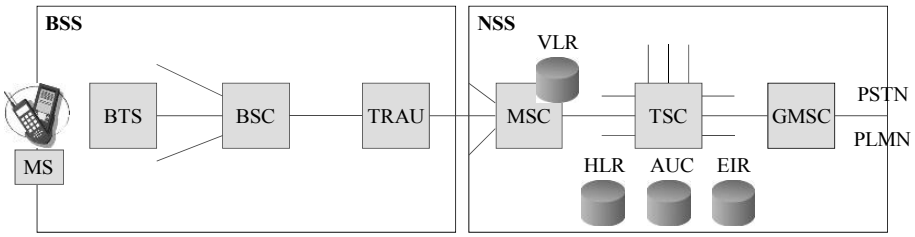


Figure 1.1. *Architecture of the GSM network*

Different types of equipment in the mobile network are able to interface at a rate of 2,048 kbps. This rate is the result of time-division multiplexing of 32 channels or time-slots at 64 kbps, numbered 0 to 31. The first time-slot is used for synchronization of the digital frame and for monitoring the quality of the time-division multiplex. The other time-slots are appointed to signaling or traffic channels. The link between the different pieces of network equipment is ensured by a transmission network.

The user can move about within the territory covered by the GSM network. He or she must therefore be able to call and be called, and this network must register the LAI (Location Area Identification) where the mobile is situated: this is the notion of roaming. The mobile is in contact with a BTS that covers an area called a cell. The connection between the mobile and the network must be maintained while moving, which entails a change of cell; this is the notion of mobility or handover.

1.2.2. *The mobile*

The MS is the piece of equipment given to the user to establish the connections to carry speech and data in order to exchange SMS messages. The MS contains terminal equipment and a SIM (Subscriber Identity Module) card.

Each piece of terminal equipment is uniquely identified by an IMEI (International Mobile Equipment Identity) number allocated by the manufacturer. The SIM card identifies the user and is used to establish the communication. The portability of the SIM card means that all types of terminal can be used to establish a communication. The SIM card contains the IMSI (International Mobile Subscriber Identity) number that identifies the subscriber, and this is only known within the GSM network.

1.2.3. *The radio sub-system*

1.2.3.1. *The physical architecture*

The BTS is a set of transmitters and receivers in charge of radio transmission with mobiles (modulation, error-correcting code, time-division and frequency-division multiplexing). It is used to access the physical layer. It provides:

– access to a frequency band in FDMA (Frequency Division Multiple Access) mode;

– access to a time-slot in TDMA (Time Division Multiple Access) mode.

It carries out all radio measures that will be used to verify the correct execution of a communication.

The type and location of the BTS determines the surface of the cells. In a rural area, which has low-density traffic, the BTS can be restricted to a single carrier wave coupled with an omnidirectional antenna, thus covering macrocells whose range can reach 30 km (Figure 1.2).

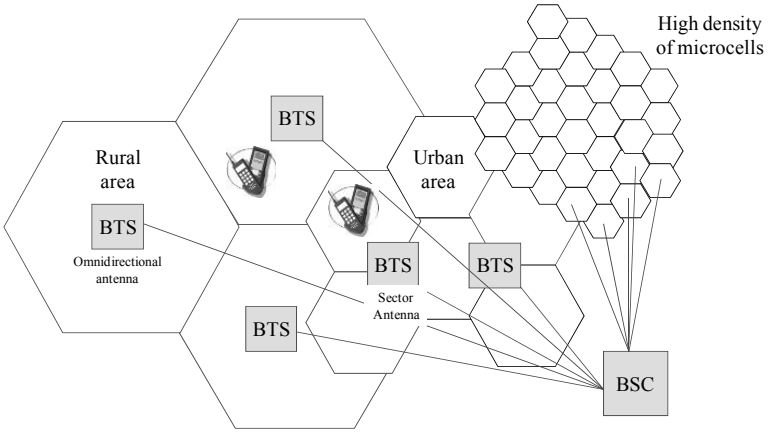


Figure 1.2. *The physical architecture of the radio sub-system*

In an urban area, which has high-density traffic, a BTS generally has several carriers coupled on sector antennas that are capable of transmitting at an angle. When the traffic density increases, microBTS − which are in charge of highly restricted or microcell areas and whose range is limited to 300 meters − are used (Figure 1.2).

The BSC controls the BTS in the sense that it manages the allocation of the RR (the frequency band and time-slot allocated to the mobile). It uses radio measurements carried out by the BTS to control the power emitted by the mobile. It decides whether to carry out a handover while the mobile changes cells.

The TRAU is a device that deals with speech transcoding. It is generally placed within proximity of the MSC, although functionally it is a part of the BSS. It is used to convert the G.711 format at 64 kbps into the format used in the radio sub-network:

– FR (full rate) at 13 kbps;

– EFR (enhanced full rate) at 12.2 kbps;

– HR (half rate) at 5.6 kbps.

The TRAU conducts the rate conversion (<14,400 kbits) of the data service to adapt it to the circuit at 64 kbps switched by the NSS.

1.2.3.2. *Protocol architecture*

Protocol architecture signals transport between the different pieces of equipment in the BSS network. This corresponds to the exchange of messages based on various communication protocols (Figure 1.3).

The function of the RR is to establish, maintain and release a channel between the MS and the BSC. Message exchange concerns the establishment and release of the radio channel, the handover, encryption activation, system information (frequency hopping, emission power control and cut-off during silences) and the indication of an incoming call (paging). The exchanges take place between the mobile and the BTS or the BSC (Figure 1.3).

Table 1.2 contains the list of RR messages.

Message type	RR messages
Radio channel establishment	ADDITIONAL ASSIGNMENT
	IMMEDIATE ASSIGNMENT
	IMMEDIATE ASSIGNMENT EXTENDED
	IMMEDIATE ASSIGNMENT REJECT
Encryption	CIPHERING MODE COMMAND
	CIPHERING MODE COMPLETE
Handover	ASSIGNMENT COMMAND
	ASSIGNMENT COMPLETE
	ASSIGNMENT FAILURE
	HANDOVER COMMAND
	HANDOVER COMPLETE
	HANDOVER FAILURE
	PHYSICAL INFORMATION
Radio channel release	CHANNEL RELEASE
	PARTIAL RELEASE
	PARTIAL RELEASE COMPLETE
Paging	PAGING REQUEST
	PAGING RESPONSE
System information	SYSTEM INFORMATION TYPES 1 to 8
Various	CHANNEL MODE MODIFY
	RR STATUS
	CHANNEL MODE MODIFY ACKNOWLEDGE
	FREQUENCY REDEFINITION
	MEASUREMENT REPORT
	CLASSMARK CHANGE
	CLASSMARK ENQUIRY

Table 1.2. *The RR messages*

The MM function is in charge of mobile location, its authentication and the allocation of a TMSI (Temporary Mobile Subscriber Identity) to replace the

IMSI identity. The exchanges take place between the mobile and the MSC (Figure 1.3).

Table 1.3 contains the list of MM messages.

Type of message	MM messages
Location registration	IMSI DETACH INDICATION
	LOCATION UPDATING REQUEST
	LOCATION UPDATING ACCEPT
	LOCATION UPDATING REJECT
Security	AUTHENTICATION REQUEST
	AUTHENTICATION RESPONSE
	AUTHENTICATION REJECT
	IDENTITY REQUEST
	IDENTITY RESPONSE
	TMSI REALLOCATION COMMAND
	TMSI REALLOCATION COMPLETE
Connection management (CM)	CM SERVICE ACCEPT
	CM SERVICE REQUEST
	CM SERVICE REJECT
	CM SERVICE ABORT
	CM REESTABLISHMENT REQUEST
	ABORT
Various	MM STATUS

Table 1.3. *MM messages*

The CM (Communication Management) function is in charge of the establishment, maintenance and release of the call, the management of additional services such as call waiting, call transfer and SMS transmission indication. The exchanges take place between the mobile and the MSC (Figure 1.3).

Table 1.4 contains the list of CM messages.

Type of message	CM messages
Call establishment	ALERTING
	CALL PROCEEDING
	CALL CONFIRMED
	CONNECT
	CONNECT ACKNOWLEDGE
	EMERGENCY SETUP
	PROGRESS
	SETUP
Call information	MODIFY
	MODIFY COMPLETE
	MODIFY REJECT
	USER INFORMATION
	HOLD
	HOLD ACKNOWLEDGE
	HOLD REJECT
	RETRIEVE
	RETRIEVE ACKNOWLEDGE
	RETRIEVE REJECT
Call release	DISCONNECT
	RELEASE
	RELEASE COMPLETE
Various	CONGESTION CONTROL
	NOTIFY
	STATUS
	STATUS ENQUIRY
	START DTMF
	STOP DTMF
	STOP DTMF ACKNOWLEDGE
	START DTMF REJECT
	FACILITY

Table 1.4. *The CM messages*

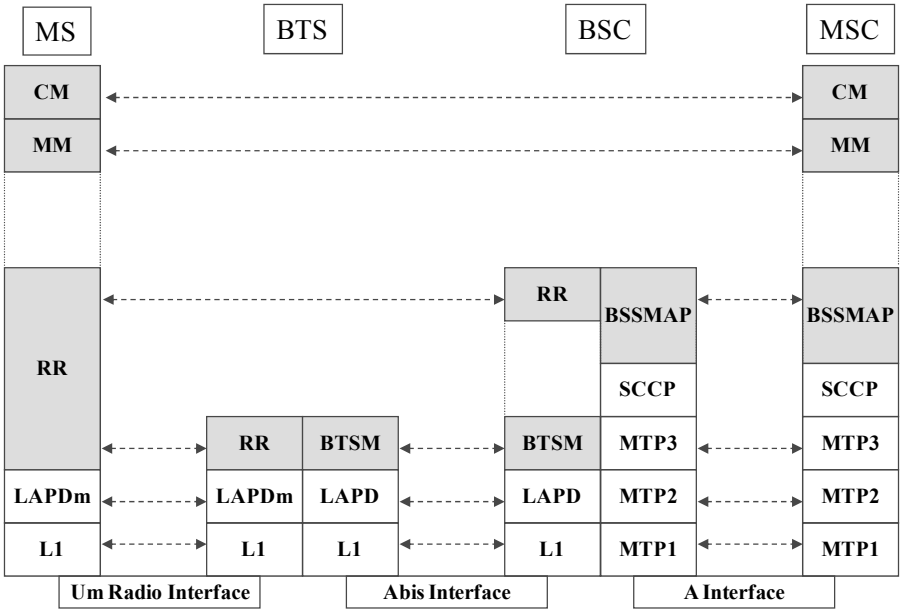


Figure 1.3. *Protocol architecture of the BSS*

At BTS level, the distribution layer specifies two types of message:

– the transparent messages that contain CM, MM and RR signaling exchanged between the mobile and the BSC or the MSC, for which the BTS acts solely as a relay;

– BTSM (BTS Management) messages corresponding to exchanges between the BTS and the BSC.

Transparent messages contain the following fields:

– the type of message, specifying whether transmission on the radio interface is in connected mode or not;

– the number of the time-slot (in the TDMA frame and eventually in multi-frame) used on the radio interface;

– the connection identifier giving the type of logical channel on which the message must be transmitted and the type of message, in order to position the SAPI (Service Access Point Identifier) of the LAPDm (Link Access Protocol – Channel D mobile) protocol.

The BTSM function defines the dialog between the BSC and the BTS (Figure 1.3). The main messages exchanged concern call procedures from the mobile or network, activation and deactivation of the RR and the change of mobile cells. This function is also used to recover the radio measurements made and to control the levels of power emitted by the BTS.

At BSC level, there are two types of BSSAP (BSS Application Part) message:

– the messages interpreted by the BSC relating to RR management, supported by the BSSMAP (BSS Management Application Part) sub-layer;

– the (CM and MM) messages supported by the DTAP (Direct Transfer Application Part) sub-layer for which the BSC ensures a relay function.

To differentiate between the BSSMAP and DTAP sub-layers used at BSSAP protocol level, there is a distribution sub-layer that acts as a protocol discriminator.

The BSSMAP function defines the relationship between the MSC and BSC (Figure 1.3). The main messages exchanged concern the availability of RR queries, the broadcast request for a mobile call within a location area, the request for the establishment or release of a radio channel, the execution of a handover and transmission in encrypted mode.

The DTAP protocol sends the CM and MM messages that are received without interpreting the contents. It contains a DLCI (Data Link Connection Identification) identifier which gives the SAPI used on the radio channel.

LAPD (Link Access Protocol − Channel D) is a data-link protocol running in asynchronous mode balanced between the BTS and the BSC (Figure 1.3). This mode is balanced because there is no master−slave relationship. Each station can initialize, control and correct errors and send frames at any time. The LAPD has three types of frame:

– the information frame used for acknowledgement and dataflow control;

– the supervision frame used for acknowledgement and flow control in the absence of traffic;

– the unnumbered frame used for information transfer without acknowledgement and without control or to open or close the connection.

The LAPDm is an adaptation of the LAPD running between the BTS and the mobile (Figure 1.3). It is characterized by a frame of fixed length. The LAPD addresses contain the TEI (Terminal End point Identifier) which identifies the pair of BTS and SAPI radio transmitter/receivers indicating the type of data encapsulated. The LAPDm protocol only retains the SAPI.

1.2.4. *The network sub-system*

1.2.4.1. *The physical architecture*

The MSC carries out the time division switch of circuits at 64 kbps. It manages to establish communication thanks to signaling messages exchanged between the MS and the entities of the NSS. It transfers SMS text messages and executes the handover when necessary.

The GMSC is a particular type of MSC that conducts the interface either with the PSTN fixed-line telephone network or with another PLMN mobile network when this cannot query the HLR. It is used to establish a call being received by the MSC to which the mobile is connected.

The TSC carries out the time-division switch of circuits at 64 kbps involving the transmission between two MSC switches. It introduces a hierarchy to the establishment of channels at 64 kbps with the purpose of optimizing the number of links with the MSC.

The VLR is a database that memorizes the data of the user present in the geographical area covered by one or more MSCs. The data stored by the VLR come partly from the HLR. It is completed by the TMSI, the MSRN (Mobile Station Roaming Number) allocated to the user in the network sub-system and by information regarding the mobile's location (LAI).

Within an area managed by a VLR, a subscriber has a temporary identity, the TSMI, allocated by the VLR to the MS. To avoid an intruder intercepting the IMSI, this is only transmitted when the device is switched on. Subsequently, only the TMSI is transmitted on the radio link. The allocation of a new TMSI occurs, at a minimum, each time the VLR changes, and possibly at the request of the mobile.

The HLR is a database that manages the details of each subscriber:

– the subscriber's IMSI used by the network;

– the subscriber's directory number (his or her MSISDN or Mobile Station ISDN Number), known outside the network;

– the subscription profile, such as additional services or the authorization of an international call.

The HLR is also a location database. It records the number of the VLR where the mobile was recorded, even when the mobile is connected to a foreign network. Each subscriber's data are stored in a single HLR, independent of its location.

A GSM network can contain one or more HLRs, depending on the number of subscribers, the capacity of the HLR and the organization of the network. To identify an HLR in the case of call processing, the MSC uses the MSISDN or the IMSI to consult the virtual HLR where the correspondence between the identity of the subscriber and his or her HLR is recorded.

The AuC is a database that memorizes a secret key used to authorize the user and to encrypt communications for each subscriber. It is generally connected with the HLR and all can be integrated into the same device.

The EIR is a database that contains the IMEI of the terminal piece of equipment. It is consulted when there are connection requests from a user. It can contain a white list of all approval numbers shared by all terminal numbers in the same series, a black list of stolen or prohibited terminals, and a grey list of terminals that have insufficient malfunctions to justify a complete interdiction.

1.2.4.2. *The protocol architecture*

The signaling network Signaling System 7 is a data network that transports messages exchanged between network sub-system equipment and uses the ISUP (ISDN User Part) protocol for call processing, the MAP (Mobile Application Part) protocol for roaming and MM and the INAP (Intelligent Network Application Part) protocol for querying a service control point.

The Signaling System 7 network consists of the signaling points hosted by the network sub-system's equipment. These signaling points can communicate via the signaling transfer points, which carry out packet forwarding.

1.2.4.2.1. The ISUP protocol

The ISUP protocol defines the procedures used to configure, manage and release the circuits that transport vocal signals and data. The ISUP message data are encapsulated by the MTP3 header or the SCCP header (Figure 1.4).

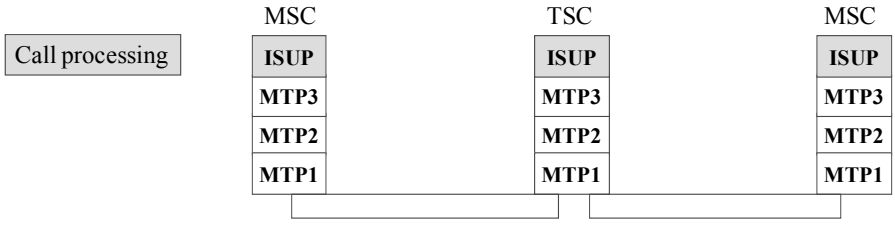


Figure 1.4. *The ISUP protocol*

The main ISUP messages are used to establish and release communication:

– the Initial Address Message is transmitted from switch to switch to communicate the request to establish a communication. It contains the telephone numbers of the user making the request and the user being requested, as well as the service type (voice, data);

– the address complete message is returned by the incoming switch to indicate that the alert has been activated;

– the answer message is transmitted by the incoming switch to indicate that the user being requested has picked up his or her phone;

– the release message is sent to release resources when a user hangs up his or her telephone;

– the release Complete message is transmitted to acknowledge the release message.

1.2.4.2.2. The MAP protocol

The MAP protocol defines the procedures for the authorization of users, the identification of devices, and roaming management. MAP message data are encapsulated by a TCAP header (Figure 1.5).

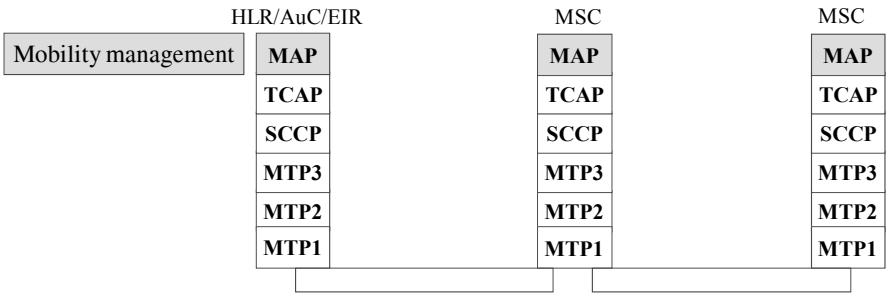


Figure 1.5. *The MAP protocol*

The MAP messages are used to create a dialog between the MSC and the HLR/AuC to fulfill the following functions:

– the recovery of mobile authentication data;

– the recovery of the subscriber's profile data;

– to find the location of the mobile (VLR number);

– to relay information between the GMSC and the MSC during an incoming call.

Interface	Links	Use
A	MSC – BSC	Incoming and outgoing call and signaling exchanges
B	MSC – VLR	Incoming and outgoing call exchanges
C	GMSC – HLR	Query of the HLR during the incoming mobile call
D	VLR – HLR	Management of user data concerning security and location
E	MSC – MSC	Handover of inter-MSC exchanges
F	MSC – EIR	Verification of terminal identity
G	VLR – VLR	Handover of inter-MSC exchanges
H	HLR – AuC	Authorization data exchanges

Table 1.5. *Interfaces using the MAP protocol*

1.2.4.2.3. The INAP protocol

The INAP protocol defines the messages exchanged between the components of the intelligent network (Figure 1.6):

– SSP (Service Switching Point). This function is integrated into the telephone switch. It is the trigger point for invoked services;

– SCP (Service Control Point). This function contains the service logic and is located in a service platform that is invoked by the SSP function.

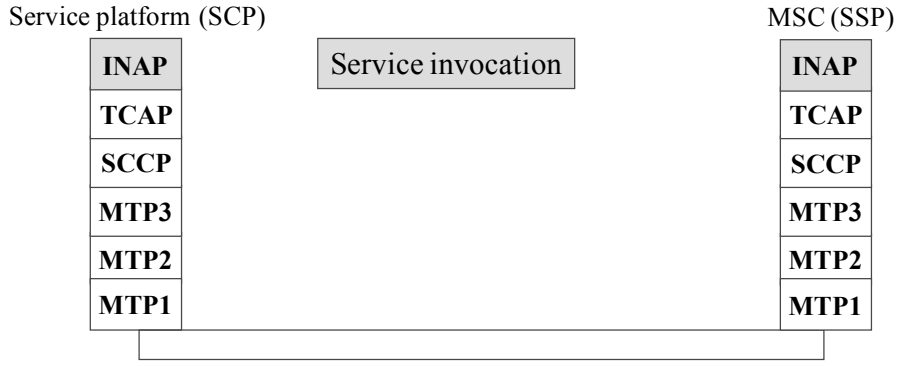


Figure 1.6. *The INAP protocol*

The extension of the INAP protocol to mobile networks is called CAMEL (Common Architecture for Enhanced Mobile Logic). The CAP (CAMEL Application Part) protocol is a sub-assembly of the INAP protocol. It is used to offer services in prepaid mode, short number services such as calling voicemail, and Virtual Private Network services.

1.2.4.2.4. The TCAP protocol

The TCAP (Transaction Capabilities Application Part) protocol divides into two distinct layers: the transactional part and the component part.

The transactional part manages the states of the dialog and the connection between the two signaling points. The structured dialog is used to start up a dialog, exchange the components within this dialog, terminate a dialog or abandon it. No triggering is associated with an unstructured dialog.

The component part, encapsulated by the transactional part, manages the type of information exchanged. An operation invocation requests that an action be carried out by the remote extremity. The response indicates whether the execution of the operation has succeeded or failed.

1.2.4.2.5. The SCCP protocol

The SCCP (Signaling Connection Control Part) protocol provides the control functions from start to finish between two signaling points. Several modes are defined:

– connectionless mode;

– connectionless mode with resequencing;

– connection mode;

– connection mode and flow control.

The SCCP protocol also provides an address translation function called Global Title. The SCCP gateway translates this Global Title into a code point (MTP3 address) and a Sub-System Number that identifies the application protocol.

1.2.4.2.6. The MTP protocol

The MTP (Message Transfer Part) protocol carries out message transfer. It consists of three layers MTP1, MTP2 and MTP3 corresponding to physical, data link and network layers, respectively.

The MTP3 layer is used for routing messages at the signaling transfer point (STP in Figure 1.7). It is in charge of re-routing the signaling channel when the physical link is cut or when there is congestion in the network.

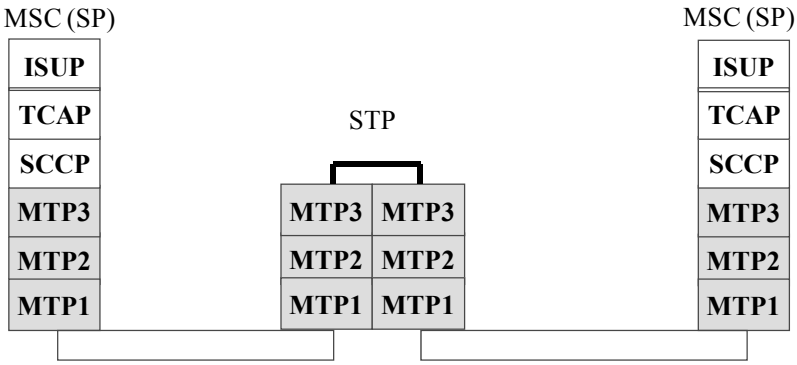


Figure 1.7. *MTP3 routing*

The MTP2 layer ensures the reliable transfer of the MTP3 packet between two adjacent nodes. It includes flow control, message sequence validation and error detection. If there is an error, the message is retransmitted.

The MTP1 layer corresponds to circuits at 64 kbps that are exchanged between the equipment and the signaling transfer points. These circuits are multiplexed in a link at 2 Mbps, and transported by the transmission network.

1.3. The radio interface

1.3.1. *The transmission chain*

The transmission chain includes all operations carried out on speech, data and signaling signals (Figure 1.8):

– source coding for speech or adaptation of the bit rate for data[1];

– channel coding for all information to be transmitted;

– constitution of the time-slot, time-division multiplexing entity;

– encryption;

– modulation.

1 Chapter 2 deals solely with source coding for speech.

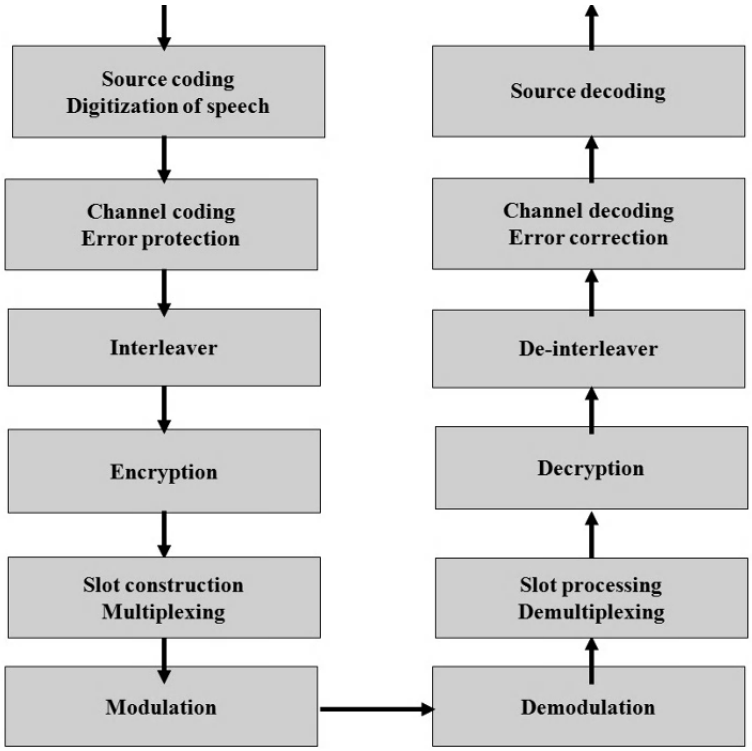


Figure 1.8. *The transmission chain*

1.3.2. *Source coding*

1.3.2.1. *Codecs*

The first stage of speech digitization consists of signal sampling at 8 kHz, which is used to obtain a sample every 125 µs. Each sample is then quantified on 13 bits to obtain a digital signal at 104 kbps. The codec's role is to reduce the source's bit rate. It functions on blocks of 20 ms, equating to 160 samples per block.

The FR coder transforms the block of 160 samples into a block of 260 bits, which corresponds to a bit rate of 13 kbps.

The EFR coder transforms the block of 160 samples into a block of 244 bits, which corresponds to a bit rate of 12.2 kbps.

The HR coder transforms the block of 160 samples into a block of 112 bits, which corresponds to a bit rate of 5.6 kbps.

1.3.2.2. *Discontinuous transmission*

For voice communications, it is rare that the two individuals will speak simultaneously. Furthermore, speech characteristics reveal very short silences between words. In fact, on average, speech constitutes only 40% of the length of the communication. Two modes of transmission can be distinguished:

– speech transmission when the user is speaking;

– the transmission of comfort noises during silences.

DTX (Discontinuous Transmission) consists of interrupting the transmission during silences and has the following advantages:

– a reduction in battery consumption of a mobile, which means that there is an increase in autonomy;

– a decrease in the average level of interference generated, which means that frequencies are reused more efficiently.

When DTX mode is used, it is necessary to distinguish the noise signal. This is the role of the Voice Activity Detector, which calculates certain signal parameters (energy, frequency) every 20 ms and compares them with thresholds in order to make a decision.

1.3.3. *Channel coding*

1.3.3.1. *Error correcting codes*

The size of the speech block delivered by the FR codec is 260 bits over 20 ms. The channel coding applied depends on the type of bits used (Figure 1.9):

– Class II 78 bits are not protected. If an error occurs in the field, their loss does not induce a significant deterioration in speech quality.

– Class Ia 50 bits are the most important bits. They are subject to dual protection, by a cyclic code and a convolutional code.

– Class Ib 132 bits are subject to protection by the same convolutional code as the class Ia bits.

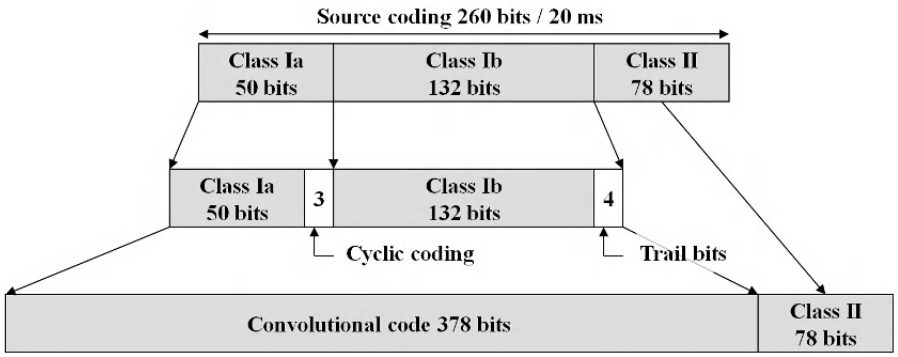


Figure 1.9. *Channel coding – the FR codec*

Table 1.6 summarizes the error-correcting codes used for different logical channels. The TCHs (traffic channels) are used to transport traffic (speech or data). The other channels transport signaling messages.

Logical channel	Size of incoming block (bits)	Channel coding	Size of outgoing block (bits)
TCH codec FR	50 132 78	Cyclic (3) + convolutional 1/2 Convolutional 1/2 None	456
TCH codec EFR	65	Preliminary coding: cyclic (8) + repetition(8) Coding identical to that of the FR	456
1/2 TCH codec HR	22 73 17	Cyclic (3) + convolutional (1/3) Convolutional (1/3) None	228
SCH	25	Cyclic (10) + convolutional (1/2)	78
RACH	8	Cyclic (6) + convolutional (1/2)	36
FACCH, SDCCH, SACCH, BCCH, PCH, AGCH	184	Fire code (40) + convolutional (1/2)	456

Table 1.6. *The coding of different logical channels*

1.3.3.2. *Interleaving*

Interleaving is a technique used to protect the receiver against surges in errors. It consists of spreading bits before their transmission on the radio channel by fragmenting error packets and allowing a greater efficiency of correction by the convolutional code. The main disadvantage of interleaving is the resulting delay that lowers the speech quality.

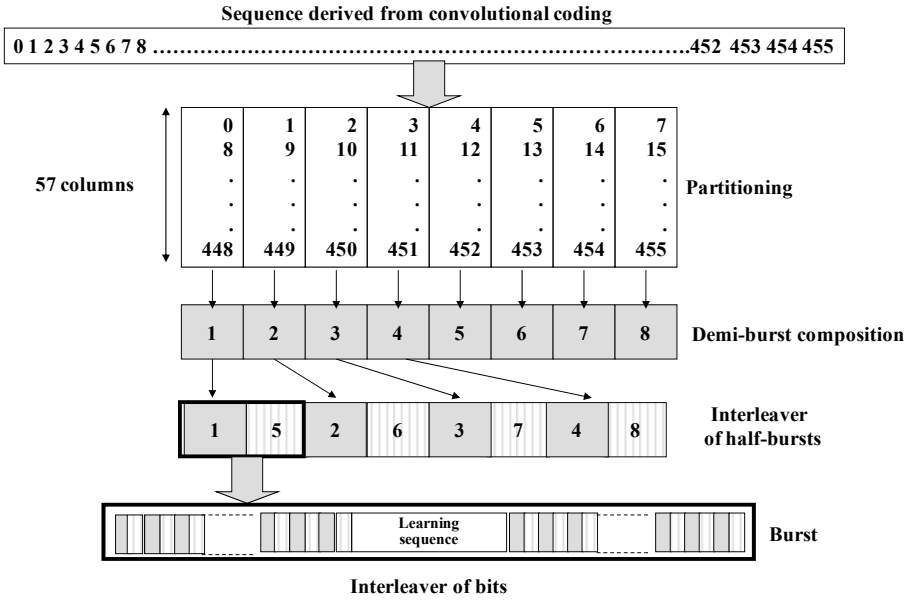


Figure 1.10. *Interleaving*

The block of speech bits (either FR or EFR) provided by the convolutional code has a length of 456 bits. The bits are returned line-by-line in a table of 57 lines and eight columns. The block is then read column-by-column and each column of 57 bits corresponds to a half-burst. The initial block is therefore cut into eight half-bursts (Figure 1.10).

Each half-burst of a block is therefore associated with the half-bursts of the preceding block (for 0, 1, 2 and 3 half-bursts) or with the half-bursts of the following block (for 4, 5, 6 and 7 half-bursts). A time-slot contains a half-burst of one block and a half-burst from the block preceding or following it (Figure 1.10).

The last stage consists of interleaving the half-bursts of the two different blocks inside the slot at the bit level. Thus the paired bits of the burst correspond to the most recent block and the odd bits to the preceding block (Figure 1.10).

1.3.4. *Time-division multiplexing*

1.3.4.1. *The structure of multiplexing*

The TDMA frame is formed from eight slots. On a frequency pair, a particular slot or half slot is appointed to a mobile link, according to the source coding used. This pair of slots constitutes a physical channel that supports various logical channels. The logical channel is therefore defined as the assignment of part of the physical channel to a particular function:

– a traffic function for the transfer of speech or data channels;

– a signaling function for call establishment and the processing of additional services;

– a time and logic synchronization function between the mobile and the BTS;

– a function of parameter measurements linked to radio propagation;

– a function of network access control.

The physical channel consists of eight time-slots or slots numbered from 0 to 7. A set of slots with the same number is called a multi-frame. There are two types of multi-frame: the 26-slot multi-frame and the 51-slot multi-frame. Each multi-frame transports several logical channels. A logical channel is identified by one or more slot numbers in the multi-frame (Figure 1.11).

The super-frame is a structure common to two types of multi-frame. It consists of 26 multi-frames of 51 slots, or 51 multi-frames of 26 slots. The super-frame has no particular significance (Figure 1.11).

The hyper-frame is an assembly of 2,048 super-frames, that is to say 2,715,648 slots. Each of the TDMA frame's slots can be found by a FN (Frame Number) frame counter. The BTS regularly sends the FN counter to the mobile, allowing it to locate itself in the hyper-frame. This counter is used for encryption of the link and for tracking system information (Figure 1.11).

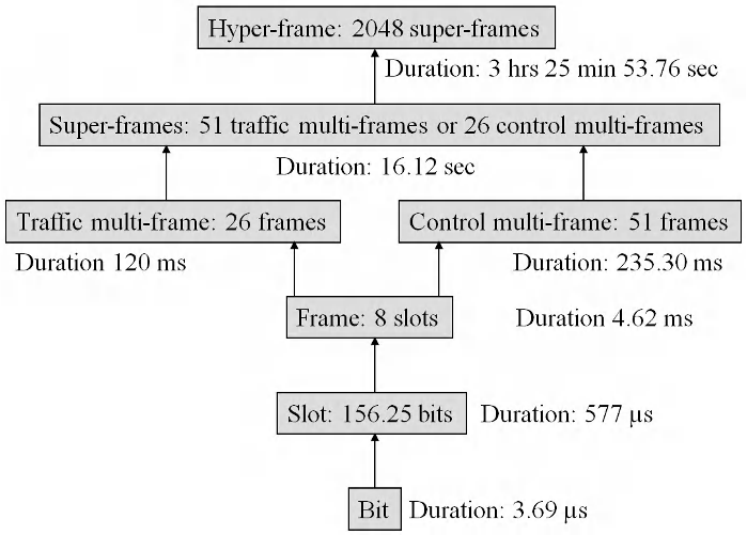


Figure 1.11. *The structure of time-division multiplexing*

1.3.4.2. *The structure of bursts*

A burst is transmitted to the interior of a slot. There are four types of burst:

– the normal burst, used for the following logical channels:

TCH (Traffic CHannel),

FACCH (Fast Associated Control CHannel),

SACCH (Slow Assisted Control CHannel),

SDCCH (Stand-alone Dedicated Control CHannel),

BCCH (Broadcast Control CHannel),

PCH (Paging CHannel) and

AGCH (Access Grant CHannel);

– the access burst used for the logical channels RACH (Random Access CHannel) and FACCH during a handover operation;

– the frequency correction burst used for the logical FCCH (Frequency Correction CHannel);

– the synchronization burst used for the logical SCH (Synchronization CHannel).

Each burst contains the following fields:

– a header and a tail-end: bits at zero at the beginning and end of the burst used to avoid the loss of synchronization;

– control of traffic data bits;

– a training sequence to model the transmission channel.

The training sequence fulfills the following functions:

– determines the position of the desired signal in the burst;

– evaluates transmission channel distortion;

– distinguishes between two cells using the same frequency.

1.3.4.2.1. The structure of the normal burst

A normal burst contains the following fields (Figure 1.12):

– a header and a tail-end, each consisting of 3 bits, used to avoid synchronization loss;

– information consisting of two sequences of 57 bits, containing traffic or signaling data;

– the 2-bit flag, indicating whether the information is regarding traffic or signaling;

– a training sequence of 26 bits, containing a sequence known to the mobile used by the receiver to equalize the radio transmission channel;

– a guard time of 8.25 bits, which stops adjacent slots received via the BTS from overlapping.

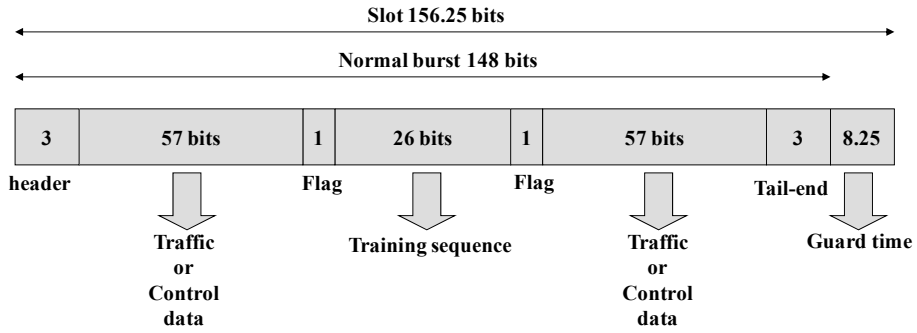


Figure 1.12. *The structure of the normal burst*

1.3.4.2.2. The structure of the access burst

The access burst has the following characteristics (Figure 1.13):

– the guard time is increased because the TA (Time Advance), used to compensate for the off-set time between mobiles, is unknown;

– the training sequence and the header are increased to improve signal detection.

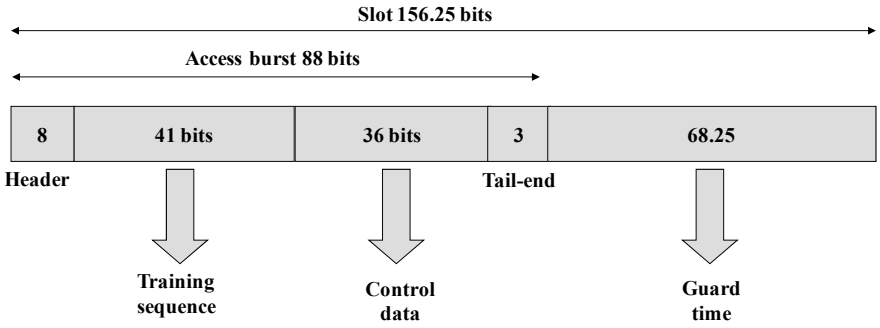


Figure 1.13. *The structure of the access burst*

1.3.4.2.3. The structure of the frequency correction burst

The frequency correction burst, used for frequency recovery, is distinctive because all bits are at zero (Figure 1.14).

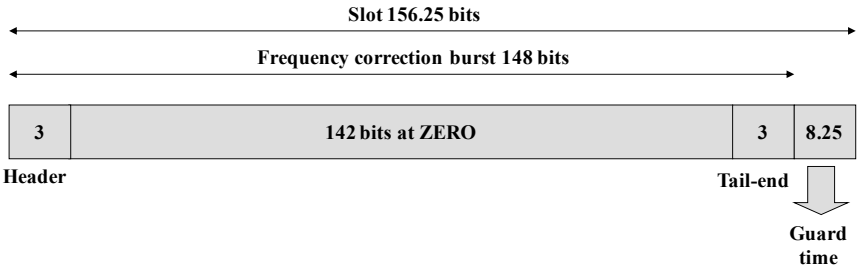


Figure 1.14. *The structure of the frequency correction burst*

1.3.4.2.4. The structure of the synchronization burst

The synchronization burst has a structure close to that of the normal burst (Figure 1.15):

– the information consists of 39 bits;

– the training sequence consists of 64 bits.

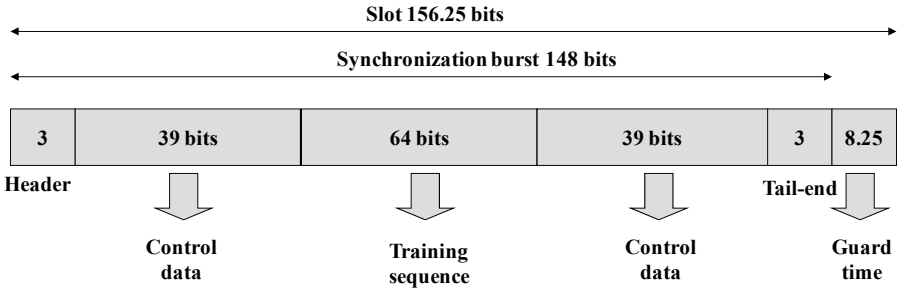


Figure 1.15. *The structure of the synchronization burst*

1.3.4.3. *Frame alignment*

The time taken for radio propagation is 3.33 μs per km, which is comparable to the duration of a binary digit in the time-division multiplex (3.7 μs). For each physical channel, the BTS waits to receive a slot on the uplink 1.730 ms after transmission on the downstream channel. Mobiles should therefore transmit with the anticipation of TA, calculated by the network and sent to each mobile (Figure 1.16).

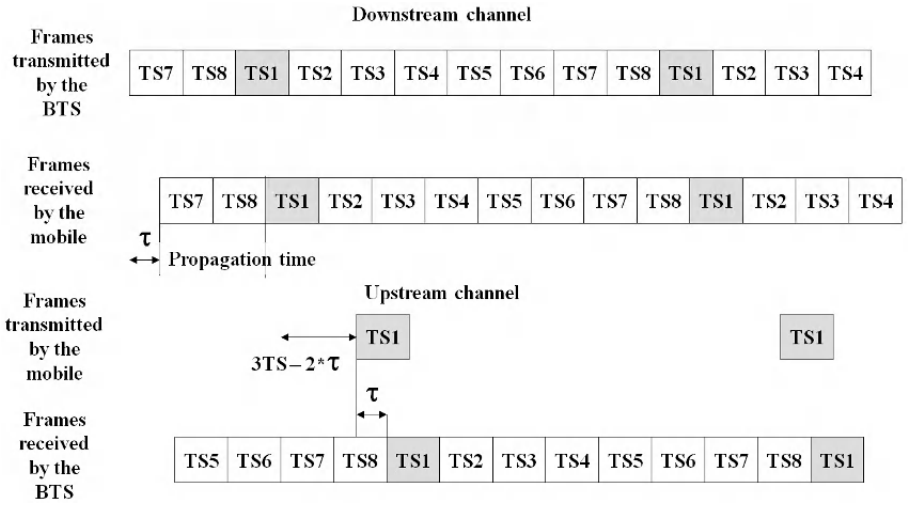


Figure 1.16. *Frame alignment*

The TA is an integer between 0 and 63, and each TA corresponds to the time of a binary digit, which is at 550 m of radio propagation. The maximum value of the TA determines the maximum radius of the cell, which is 35 km.

By using two time-slots per channel, it is possible to extend the scope. The maximum value of the TA is equal to 232 μs + 577 μs. The maximum distance between the BTS and the mobile is equal to 120 km.

1.3.4.4. *The logical channels*

1.3.4.4.1. The beacon channel

The beacon channel corresponds to a particular frequency emitted by the BTS. A mobile uses this frequency to periodically measure the signal level that it receives and to determine whether it is within the scope of the station. Each beacon channel consists of signals specific to its own synchronization and system information giving the network identity and its access characteristics.

When switched on, a mobile seeks to use the most favorable beacon channel belonging to an authorized network. When awake, it constantly monitors the signal received on this and neighboring channels. When necessary, it uses a new channel and thus changes cell. Similarly, during a communication it is not sufficient for it to maintain the link with the BTS that established the link. It periodically scans the neighboring beacon channels and creates a list of BTSs that it can accept in order to establish a handover.

The beacon channel is a group of logical broadcast channels, regrouped under the term BCH (Broadcast Channel), using slot 0 of the TDMA frame:

– the logical FCCH is used for frequency synchronization;

– the logical SCH is used for time synchronization;

– the logical BCCH is used to broadcast system information.

The FCCH is a particular burst, consisting of 148 bits at 0. It corresponds to a sinusoid signal at the frequency of f0 + 1,625/24 kHz.

The SCH is a particular burst composed of a training sequence of 64 bits, 78 bits of data and 3 bits of header and 3 bits of tail. The SCH transports two parameters of 25 bits on each burst:

– a FN on 19 bits (11 bits to determine the super-frame's number), 5 bits to determine the multi-frame's number and 3 bits to determine the five possible places 1, 11, 21, 31 and 41 in the multi-frame);

– a BSIC (Base Station Identity Code) color on 6 bits, whose role is to discriminate several short-distance BTSs that have the same frequency.

Ten bits are added to 25 bits for the CRC (cyclic redundancy check) and 4 trail bits, to form the 39-bit word. A convolutional code of 1/2 rate is applied to this last word to form a 78-bit word.

The BCCH uses a normal burst to broadcast system information. The mobile requires a certain amount of information from the network in order to connect to it:

– the LAI;

– the allocation of the BCCH slot on the neighboring cells;

– the mode of CCCH (Common Control CHannel) management;

– the control parameters;

– the cell options.

1.3.4.4.2. The common control channels

The common control channels are unidirectional channels, which can be either upstream or downstream. They form a set of logical channels grouped under the term CCCH:

– the logical RACH is used upstream for random access by the mobile;

– the logical AGCH is used downstream for the allocation of a dedicated channel;

– the logical PCH is used downstream for mobile calls;

– the logical Cell Broadcast Channel is used downstream to broadcast specific short messages.

Mobiles use the logical RACH when they want to transmit a call, send text or location messages. They send a request on a single burst to the BTS, on particular slots in “slotted aloha”-type random access.

The burst used has a shorter length than a normal burst because the mobile does not necessarily know the propagation time between the place where it is located and the BTS. The transmitted burst must insert itself into the BTS slot with out interfering with the adjacent slots. The hold-off is 252 μs, which means that distances of 35 km can be taken into account between the mobile and the BTS by taking the security margins into account.

The RACH contains 8 bits that are protected by 6 bits of CRC correction code. Using modulo 2 addition, it adds the 6 bits of BSIC color of the BTS to the 6 bits of the CRC. Four trail bits are then added and a convolutional code is applied at half rate. Together they form a 36-bit word.

The 8-bit request consists of 3 to 6 bits indicating the nature of the request and a random number that aims to limit the ambiguities when two mobiles reach the same frequency at the same time.

The logical AGCH uses a normal burst. It is used by the BTS to appoint a SDCCH to the mobile in order to identify the mobile, authorize it and determine its request.

The logical AGCH contains the description of the signaling channel. This is needed for it to be able to determine the carrier number, the slot number and the TA parameter of equalization for the propagation delay.

When the network wishes to contact a mobile for a call or text message, it broadcasts the mobile's identity on a group of BTSs from the logical PCH. The mobile responds via the cell by which it is located by a random access on the logical RACH. It is possible to call four broadcast mobiles via the same message. The logical PCH uses a normal burst.

1.3.4.4.3. Dedicated channels

Dedicated channels are either TCHs or signaling SDCCHs. On a physical channel or a slot, a TCH with its associated supervision SACCH can be positioned or eight SDCCH with their associated SACCHs. The logical FACCH is a signaling channel obtained by a preemption of the TCH. The term DCCH (Dedicated Control Channel) groups all signaling or supervision channels.

The logical SACCH uses a normal burst and supports the control information of the TCHs or SDCCHs:

– mobile emission power control;

– control of the quality of the radio link;

– the repatriation of measurements carried out on neighboring beacon channels;

– the equalization of propagation delay by the TA mechanism;

– the list of the beacon channels of neighboring cells;

– identifiers of the coverage area and the cell.

The SDCCH uses a normal burst. This is a bidirectional channel dedicated to a user. It supports dialog between the mobile and the network for user authorization, the encrypted transition command, call establishment, updating the mobile's location and exchanging SMS text messages.

The FACCH uses a normal burst and represents a capacity theft normally intended for the TCH. It is used to transmit urgent information when there is a handover. To indicate the capacity theft, the 2-bit flag (stealing bits) present on every burst on each side of the training sequence is used.

The TCH uses a normal burst and acts as support for data or speech transmission. It can be used at full or half rate. At full rate it can be used for speech coding at 13 kbps (FR codec) or 12.2 kbps (EFR codec and a maximum bit rate of 14.4 kbps for data). At half rate it is used for a speech coding at 5.6 kbps (HR codec) with a maximum bit rate of 4.8 kbps for data.

1.3.4.5. *The structure of multi-frames*

1.3.4.5.1. Multiplexing of TCH, SACCH and FACCHs

When a transmission is at full bit rate, TCHs and SACCHs are multiplexed in a multi-frame of 26 slots (Figure 1.17):

– 24 slots (slots 0 to 11 and 13 to 24) are assigned to TCH;

– one slot (slot 12) is assigned to SACCH;

– one slot (slot 26) is unassigned. This (idle) slot is used by the mobile to scan neighboring beacon channels.

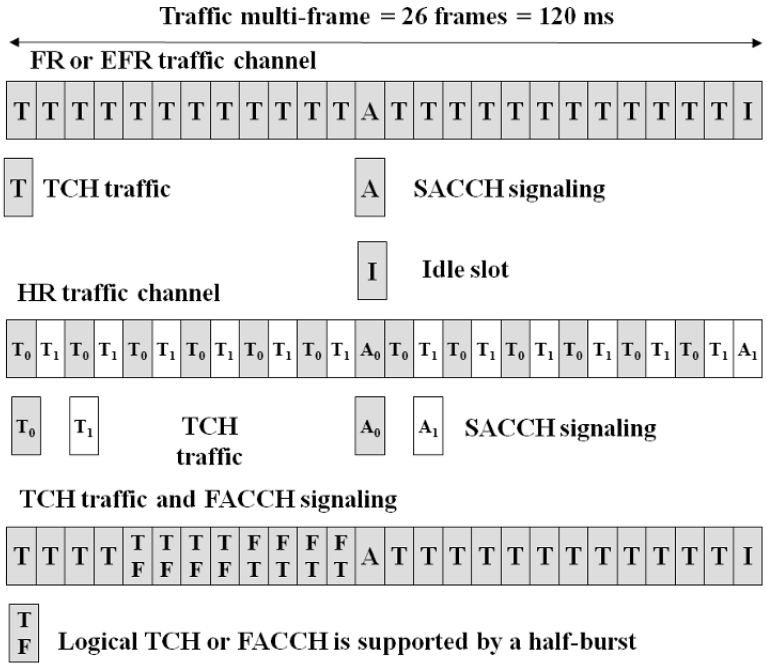


Figure 1.17. *Multiplexing of channels: TCH, SACCH and FACCH*

When a transmission is at half bit rate, a multi-frame of 26 slots supports two traffic channels. One in two slots is assigned to the traffic channel. Slots 13 and 16 are assigned to SACCHs for the supervision of the two traffic channels (Figure 1.17).

A transmitted FACCH block occupies eight half-bursts (Figure 1.17).

During a communication, the mobile takes advantage of the duration available between transmitting and receiving a burst inside the multi-frame to carry out field measurement of the neighboring beacon channels. It uses the largest duration between slot 25 of the last multi-frame and the first slot of the following multi-frame to carry out all processing operations on the neighboring BCH beacon channel (Figure 1.18).

While the mobile is being used in a communication, it uses a 26-slot multi-frame design. It analyzes broadcast channels being transmitted with a 51-slot multi-frame design. As these two numbers are first, the opening window therefore shifts to a 51-slot structure.

The same scanning principle is implemented for TCHs at half rate and for SDCCHs.

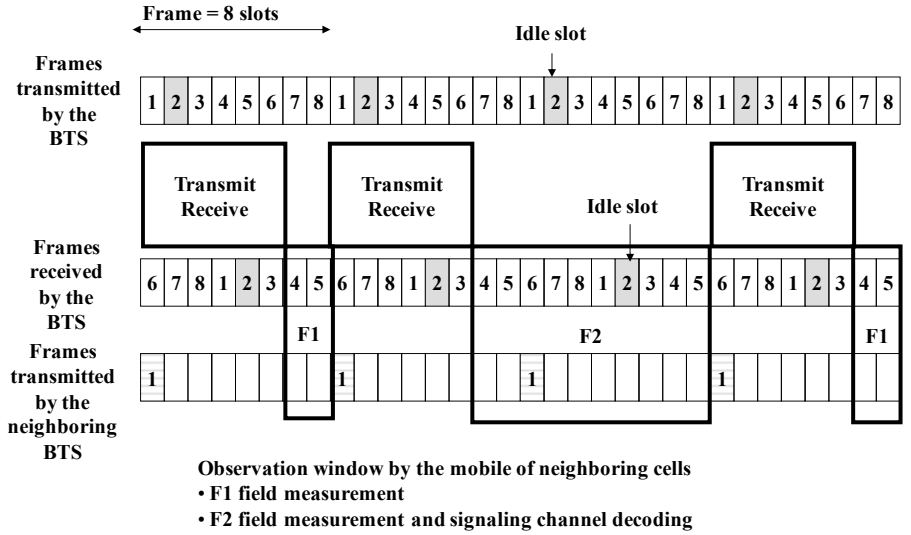


Figure 1.18. *The scanning of neighboring beacon channels*

1.3.4.5.2. Multiplexing of SDCCHs and SACCHs

SDCCHs and SACCHs are multiplexed in two 51-slot multi-frames. The upstream and downstream configurations are identical and offset by 15 frames. The physical channel merges eight SDCCHs and four SACCHs. The SDCCHs and SACCHs are transmitted on four consecutive slots in order to reduce the transmission delay of the LAPDm frame. The same physical channel is accessible to eight different users. The SACCHs are distributed on two consecutive multi-frames (Figure 1.19).

When an SMS message has to be broadcast on one or many cells, the logical Cell Broadcast Channel is used. Each message uses a block of four slots, which takes the place of a SDCCH.

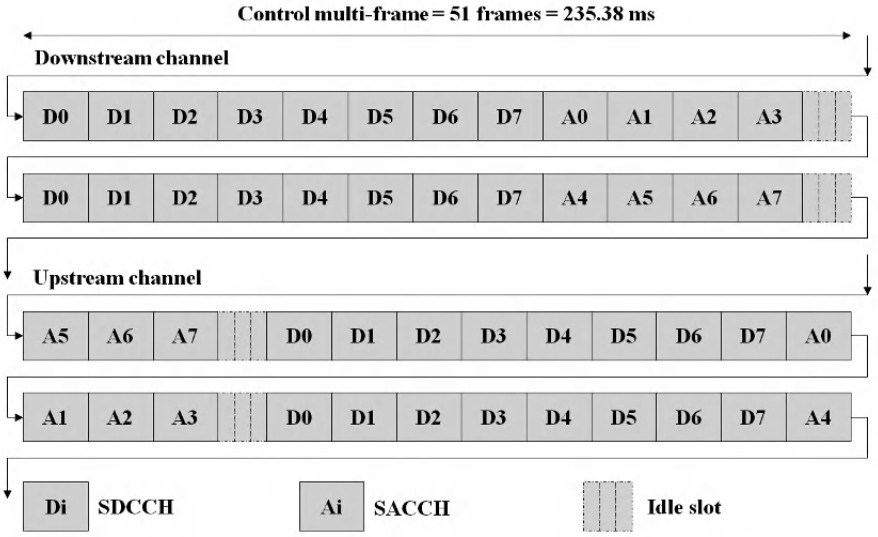


Figure 1.19. *Multiplexing of SDCCHs and SACCHs*

1.3.4.5.3. Multiplexing of the beacon channel's channels

The downstream multiplexes the FCCH, SCH, BCCH, PCH and AGCH. The FCCH is transmitted in frames 0, 10, 20, 30 and 40 of a multi-frame consisting of 51 consecutive slots. The SCH is transmitted after the FCCH. The BCCH uses the four slots of the multi-frame, numbered 2 to 5. It is possible to increase the BCCH by using four additional slots (6 to 9) when there is a large quantity of system information to broadcast (Figure 1.20).

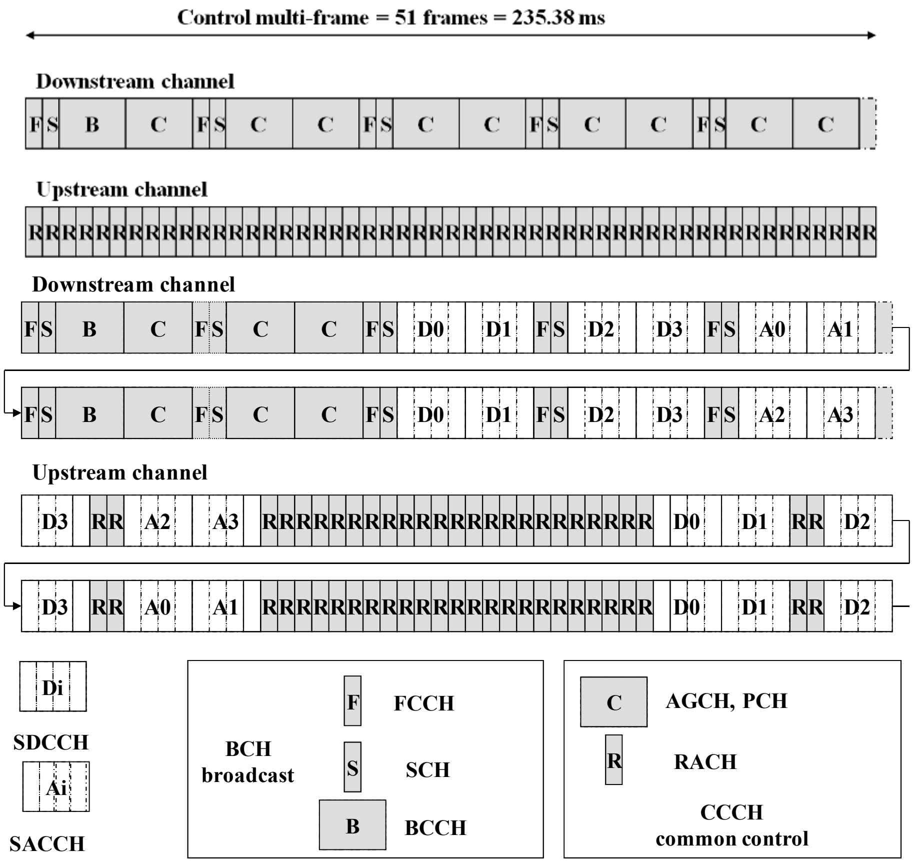


Figure 1.20. *Multiplexing the channels of the beacon channel*

The PCH and AGCH are broadcast channels that are multiplexed according to two types of configuration:

– multiplexing in a multi-frame of 51 slots with the logical broadcast channels (FCCH, SCH, BCCH). In this case, 36 slots (nine blocks of four slots) are allocated to PCH or AGCH. This case corresponds to stations of medium or high capacity (Figure 1.20);

– multiplexing in a 51-slot multi-frame with logical broadcast channels and four dedicated control channels (SDCCHs and SACCHs). In this case, 12 slots are assigned to PCHs and AGCHs. This case corresponds to stations of small capacity (Figure 1.20).

The upstream is reserved for RACH, consisting of 51 multi-frame slots (in the case of a high- or low-capacity station), or 23 slots when this multi-frame is shared with dedicated SDCCHs and SACCHs (for small capacity stations), see Figure 1.20.

1.3.5. *Modulation*

MSK (Minimum Shift Keying) is a modulation using continuous-phase frequency-hopping. The phase continuity is used to limit the spectral occupation of the modulated signal. A *fi* frequency is assigned to each binary digit: $fi = fo \pm 1/4T$, where *fo* is the central frequency of the modulated signal and *T* the rate of the binary digit.

During the binary pulse [0, T], the modulated signal is written in the form: $x(t) = A \cos [2\pi * fo * t \pm (\pi /2T) * t]$. The signal phase varies by $\pm \pi /2$ during the duration of a binary digit. At *nT* instants, the phase can take four possible 2π modulo values.

The MSK modulation uses the orthogonal frequencies *fi* and *fo*, which can obtain the best performance during a demodulation. To obtain orthogonal frequencies, the difference $(fo - fi)$ has to be a multiple of $1/2T$. The modulation index is the product $2*(fo - fi)*T$. For the MSK modulation, the modulation index is equal to 0.5.

GMSK (Gaussian MSK) modulation is a MSK modulation to which a Gaussian filter has been added following the binary digits. This low-pass filter is characterized by a *B* passing band, where *B* is the cut-off frequency at 3 dB. This filter is characterized by the product *BT*. For the GSM network, the product *BT* is equal to 0.3.

1.3.6. *The frequency plan*

The spacing between channels is equal to 200 kHz and authorizes a number of channels equal to 35 (GSM 450), 35 (GSM 480), 124 (GSM 850), 174 (GSM 900), 374 (DCS 1 800), and 299 (PCS 1900). A guard band of 100 kHz is added to the extremities of the frequency band (Table 1.7).

The cell is theoretically represented by a hexagonal structure in order to cover an area. The distance separating two cells using the same frequency must be sufficient enough to limit interference (Figure 1.21). The number of cells, *N*, that constitutes the reuse structure is given by the following formula:

$N = i^2 + i*j + j2$, *i* and *j* being integers

System	Frequency band	
	MS ⇨ BTS	**BTS ⇨ MS**
GSM 450	450.4 – 457.6 MHz	460.4 – 467.6 MHz
GSM 480	478.8 – 486 MHz	488.8 – 496 MHz
GSM 850	824 – 849 MHz	869 – 894 MHz
Standard GSM 900	890 – 915 MHz	935 – 960 MHz
Extended GSM 900	880 – 915 MHz	925 – 960 MHz
GSM 900 (railway)	876 – 880 MHz	921 – 925 MHz
DCS 1800	1710 – 1785 MHz	1805 – 1880 MHz
PCS 1900	1850 – 1910 MHz	1930 – 1990 MHz

Table 1.7. *The frequency plan*

The BSIC code transmitted in BCCH allows the mobile to differentiate two BTSs transmitting on the same frequency, from two different patterns. Similarly, the burst's training sequence type depends on the BSIC (Figure 1.21).

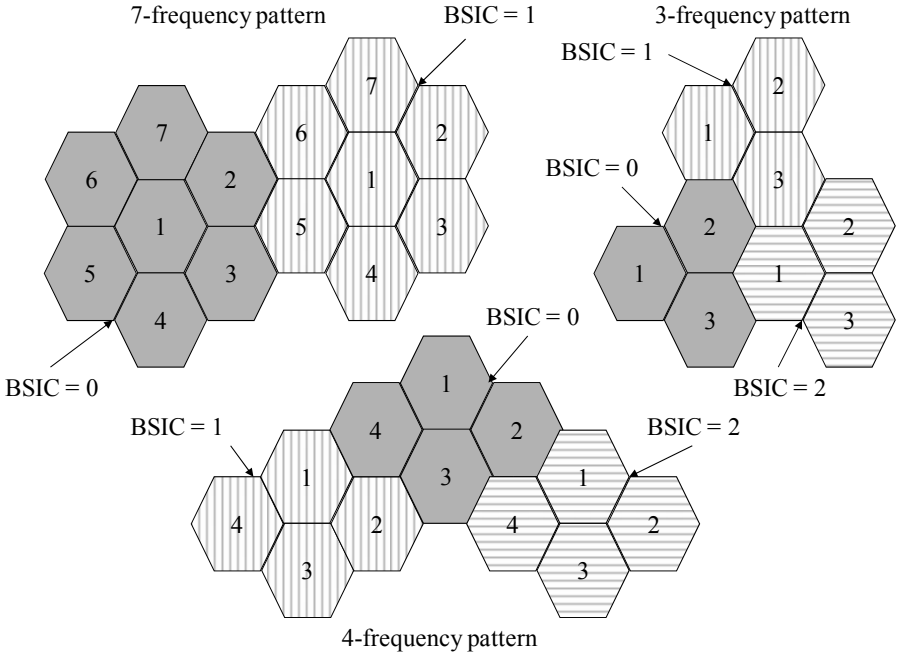


Figure 1.21. *Frequency reuse*

Frequency hopping is used to increase the system's capacity and to protect against selective fading and unwanted signals.

The radio transmission supports the slow-frequency hop and the change in frequency is carried out frame-by-frame. There are two types of frequency hop: the random hop and the cyclic hop.

Two parameters describe the frequency used for each frame:

– HSN (Hopping Sequence Number);

– MAIO (Mobile Allocation Index Offset).

The HSN parameter can take 64 values and defines the frequency sequence list to be used. If the HSN parameter is equal to 0, the frequency hop mode used is the cyclic mode. The MAIO parameter indicates the offset with regards to the frequency list, in order to identify the frequency used.

The frequencies at which the hop occurs are numbered from 0 to $N - 1$. An algorithm generates a pseudo-random series of S numbers between 1 and $N - 1$. It uses the FN and the HSN parameter as an argument.

When allocating the channel, the BSS specifies a MAIO index to the mobile, allowing it to determine the frequency to be used, by adding modulo N to the MAIO index to the S number. In the case of the cyclic hop, the value of the frequency to be used is obtained by adding the MAIO index to the frequency number.

Two different MAIO indices for the same HSN parameter define two sequences that never give the same frequencies at the same time. Two channels that have two different HSN parameters will only interfere with one in N bursts.

1.4. Communication management

1.4.1. *Establishment of the SDCCH*

The establishment procedure of the dedicated SDCCH is carried out for incoming or outgoing call establishment and when there is a location update (Figure 1.22). It starts via the transmission of a burst on the RACH transporting the RR CHANNEL REQUEST message, which contains the following information:

– a reference byte integrating a coded random number on no more than 5 bits;

– the type of service requested (allocation of a SDCCH only, of a SDCCH then of a TCH at half or full rate);

– the current FN in the hyper-frame defined by the BTS, in the form of the FN.

The BTS receives the burst, calculates the propagation delay and transfers the request to the BSC in a BTSM CHANNEL REQUIRED message. The BSC decides whether or not to accept the request depending on the RRs available.

If the response is positive, it chooses a SDCCH and possibly a TCH to allocate to the mobile. It transmits a BTSM CHANNEL ACTIVATION message, precisely describing the channel (frequency and time-slot number). The BTS reserves the channel and acknowledges this by sending the BTSM CHANNEL ACTIVATION ACKNOWLEDGE message to the BSC.

The BSC thus transmits a RR IMMEDIATE ASSIGNMENT COMMAND allocation message to the mobile via the BTS. This message, transmitted on the AGCH contains:

– the description of the dedicated channel;

– the reference byte placed by the mobile;

– the current FN;

– the value of the TA.

The mobile thus uses the dedicated SDCCH and establishes a LAPDm protocol connection, which contains the message. This message can be CM SERVICE REQUEST (for outgoing calls), RR PAGING RESPONSE (for incoming calls) or MM LOCATION UPDATING REQUEST (for locations). These messages contain the mobile's identity (IMSI or TMSI), its power rating and the service requested.

When the BTS receives the message, it transmits it to the BSC by encapsulating it in a BTSM ESTABLISH INDICATION message and acknowledges the received message on the radio channel. Connection at LAPDm protocol level is thus established.

At the same time, the BSC extracts the message contained in the BTSM ESTABLISH INDICATION message and encapsulates it in a BSSMAP COMPLETE L3 INFORMATION message. This message is acknowledged by the MSC via a SCCP CONNECTION CONFIRM segment.

A collision can occur if two mobiles transmit a request on the same RACH slot. Each mobile repeats its call having waited an integer of intervals, obtained by

random draw. This device is used to reduce successive collisions and to improve the output of the RACH.

When signals with very different levels are received, the BTS can interpret the strongest signal. The BTS therefore detects the request from one of the mobiles and transmits the allocation message on the AGCH. This message received by both mobiles contains the reference byte transmitted by the mobile, which means that both transmitters can be distinguished.

It is possible, however, that both mobiles draw the same random number. In this instance, the contention is resolved by the mobiles' identity (IMSI or TMSI) contained in the request and the response. Only the mobile that finds its identity in the response is authorized to stay on the dedicated channel. The other mobile returns to the RACH and repeats its access request.

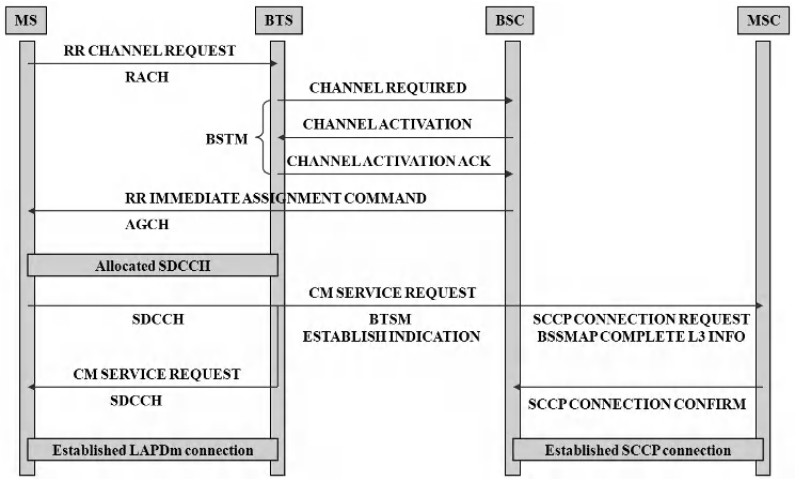


Figure 1.22. *Establishment phases of the SDCCH*

In the case of an incoming call, the allocation procedure of a dedicated SDCCH starts up by a broadcast call. The BSC sends a BTSM PAGING COMMAND message to all BTSs containing the LAI. This message contains the TMSI identity of the mobile requested. The BTS sends the RR PAGING REQUEST message on the PCH.

The mobile called must listen regularly to the PCH. When it detects the RR PAGING REQUEST message, it requests the allocation of a dedicated SDCCH for signal exchange via the RACH, by specifying that it is about a response to a paging message.

1.4.2. *Security management*

1.4.2.1. *The principals*

Use of the radio channel as a transmission support between the BTS and MSs of the cell should be accompanied by procedures to protect against fraudulent use of the network via a user authentication. It must also protect against communication interception by encrypting the data exchanged.

Implementing the authentication and encryption of information transmitted on the radio channel function the network uses the following elements:

– RAND (RANDom) numbers;

– a Ki key to authenticate and determine the Kc encryption key;

– an A3 algorithm providing a SRES number for authentication, established from the RAND number and the Ki key;

– an A8 algorithm determining the Hc key for encryption, established from the RAND number and the Ki key;

– an A5 algorithm for data encryption from the Kc key.

To avoid identity theft, the subscriber's IMSI number is only transmitted when the device is switched on. The MSC/VLR then assigns a temporary number − the TMSI that will be used during exchanges between the mobile phone and the network. The allocation of a new TMSI takes place each time the VLR changes and possibly at each mobile intervention.

Authentication is used to verify whether the identity (IMSI or TMSI) transmitted on the radio channel is correct. The authentication can be requested by the MSC/VLR for each location update and for each incoming or outgoing call establishment.

The authentication procedure implements the following exchanges between the MSC/VLR and the mobile phone (Figure 1.23):

– the MSC/VLR transmits a RAND number to the mobile;

– the mobile calculates the SRES number from the A3 algorithm and the Ki key, and then sends it to the MSC/VLR;

– the MSC/VLR compares the SRES received from the mobile to that received from the HLR/AuC. If both values are identical, the subscriber's identity is authenticated.

The encryption guarantees data privacy. The information transmitted is encrypted via the A5 and the Kc key. This key is calculated by the mobile from the RAND number, the Ki key and the A8 algorithm. It is transmitted to the BTS by the MSC/VLR (Figure 1.23).

The pieces of information necessary to authenticate the user and encrypt the data circulating on the network are grouped in the form of a triplet containing the RAND, SRES and Kc numbers. Information of a confidential nature, such as the Ki key and the A3, A5 and A8 algorithms, are stored at AuC server level and in the SIM card of the MS. Such information is not involved in transmission between the network devices.

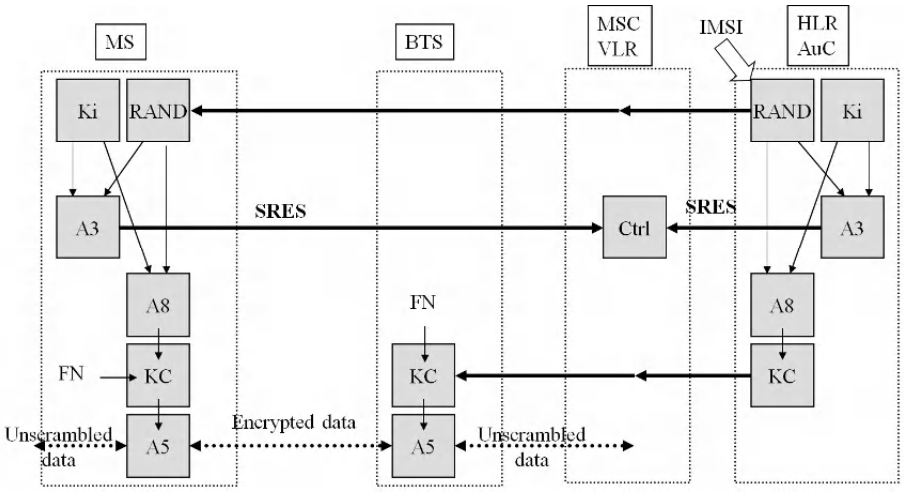


Figure 1.23. *The authentication and encryption principals*

The AuC server prepares several triplets for each mobile and transmits them to the HLR, which stores them in reserve. When the MSC/VLR needs these triplets, it requests them from the HLR indicating the mobile's IMSI number. The triplet used for authentication is destroyed and will not be used again.

1.4.2.2. *The procedures*

The AuC database prepares triplets for each subscriber; when the MSC/VLR needs these triplets, it requests them by sending a MAP SEND AUTHENTICATION INFO message. The MSC sends an authentication request to the mobile in the MM AUTHENTICATION REQUEST message, containing the RAND parameter. In its MM AUTHENTICATION RESPONSE message, the mobile sends the value of the calculated SRES (Figure 1.24).

After authentication, the MSC/VLR decides to switch to encrypted mode and sends a BSSMAP CIPHER MODE COMMAND message containing the Kc key to the BSC. The BSC then retransmits this command to the BTS in the form of a BTSM ENCRYPTION COMMAND message. The BSC sends the RR CIPHERING MODE COMMAND to the mobile to inform it of the passage in encrypted mode, and on reception activates the encryption (Figure 1.24).

When the mobile receives this message, it activates the encryption and decryption processes and acknowledges the request by sending the RR CIPHERING MODE COMPLETE message, which provokes the encryption process at BTS level. The acknowledgement message is then relayed to the MSC/VLR (Figure 1.24).

All data exchanged between the MS and the MSC/VLR will be encrypted at the level of the link between the BTS and the MS. When the mobile changes cells during a communication, the security information is sent from the previous BTS to the new one across the network in order to allow the communication to continue in encrypted mode.

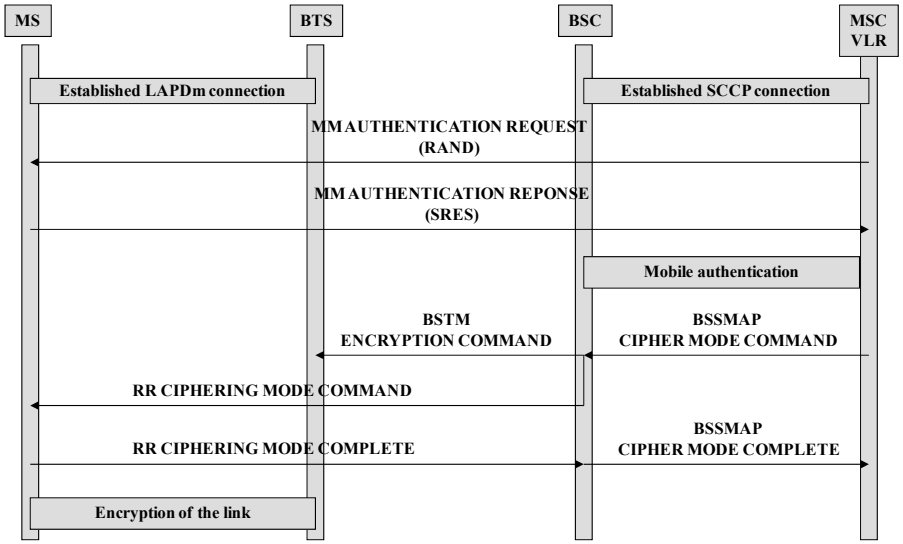


Figure 1.24. *Authentication and encryption phases*

1.4.3. *Location management*

1.4.3.1. *Principles*

A mobile that is switched on must be able to receive and transmit calls. It must select a cell and permanently monitor the beacon channels of neighboring cells to

detect an eventual change of cell. The choice of beacon is made according to criteria at the level of radio reception to guarantee an acceptable quality of service and administrative criteria in order to link up on the authorized network.

When the mobile is switched on, the cell selection process is implemented. The MS performs a selection on all frequencies available in the GSM (124 carriers) or in the DCS (374 carriers) when it has no information.

When a mobile has decoded the FCCH and SCH, it receives the number of the location area to which it belongs. A location area is identified by the location area identifier.

The LAI allows the mobile to detect location area changes, including those due to a change of network. The VLR records the current location area of all the mobiles that it manages. The HLR memorizes the identity of the current VLR of each MS.

When the mobile has recognized the beacon channel transmitted in the BCCH, using the RR protocol it will ask the MSC/VLR, a dedicated SDCCH, where the IMSI number appears unscrambled.

The MSC/VLR will initiate a procedure using the MM protocol to authenticate the mobile and then order the BTS to activate the encryption on the radio link. The MSC/VLR that recorded the MS's location area will thus be able to transmit the encrypted TMSI number to it.

The location area regroups a certain number of cells. When the mobile receives a call, the MSC/VLR will look for the mobile in the location area by communicating that it is searching. The size of the location area results from a compromise between the traffic generated by the inscription of the moving mobile and the paging message broadcast.

After selecting a location area and a network, the mobile is ready to transmit or receive calls:

– it can establish an outgoing call by using the RACH of the cell concerned; or

– it can receive an incoming call by listening to the PCH.

1.4.3.2. *Procedures*

When switched on, the MS should register with its IMSI. It sends a MM LOCATING REQUEST. The network sets up a dedicated SDCCH and the authentication procedure (Figure 1.25).

The MSC relays the information regarding the location update by transmitting the MAP LOCATION UPDATE LOCATION message to the HLR. This loads the VLR with all information concerning the user by sending the user the MAP INSERT SUBCRIBER DATA message (Figure 1.25).

The MSC/VLR can thus allocate a TMSI to the MS via the TMSI REALLOCATION COMMAND message. After the MS acknowledges this message, the location procedure is stopped by the MSC's acknowledgement of the mobile location request via the MM LOCATION UPDATING ACCEPT message. The BSS network can release the dedicated channels onto the different interfaces (Figure 1.25).

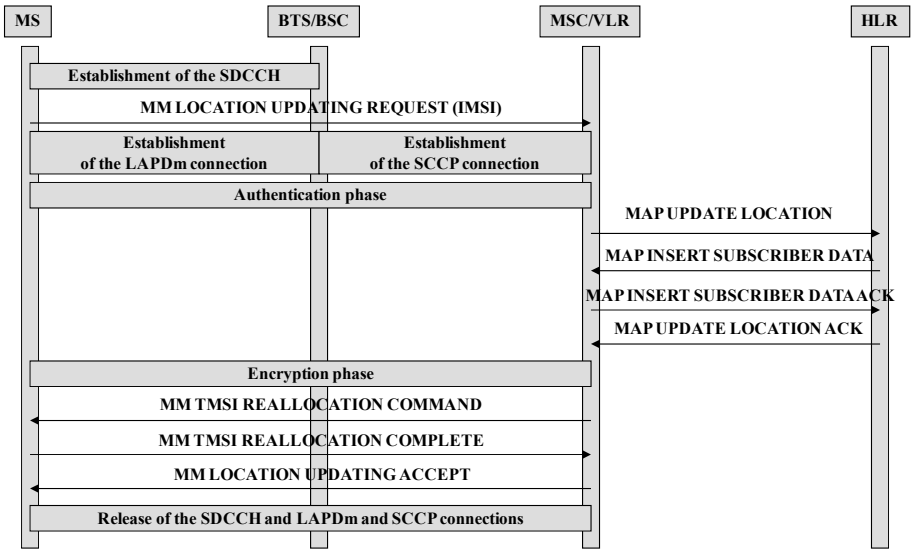


Figure 1.25. *Location phases when the device is switched on*

In the case of inter-VLR location update, the new VLR will identify the previous VLR from the previous LAI area indicated by the MS and import the information concerning the MS via the MAP SEND IDENTIFICATION message (Figure 1.26).

The new VLR can therefore initiate the MS's authentication procedure and carry out the MS's location update with the HLR. The procedure for loading data on the new VLR is identical to that previously described, when the device is switched on. The HLR also communicates with the previous VLR to delete the subscriber's data from the MAP CANCEL LOCATION message (Figure 1.26).

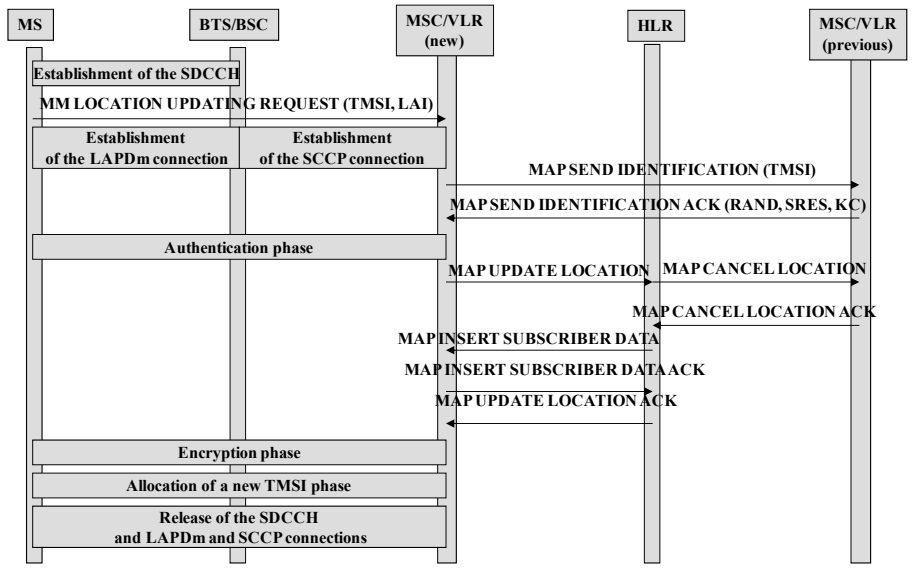


Figure 1.26. *Location phases when there is a change of VLR*

1.4.4. *Call management*

1.4.4.1. *Principals*

In the case of an outgoing call, the subscriber dials the correspondent's number and confirms his or her call by pressing a specific button. The MS initiates a procedure to request a SDCCH via which it sends a CM message containing the IMSI or TMSI of the person calling. The MSC/VLR initiates a procedure for authentication of the MS and for encryption set-up. The mobile can then transmit the number of the person being called in a CM message.

The MSC/VLR determines call delivery on the basis of the number dialed (call to another MSC, another PSTN fixed network or a PLMN mobile) by using the ISUP signaling protocol. It also orders the allocation of a TCH to a mobile. When the requested person is found and notified of a call by an alert, the MSC/VLR sends a return call tone to the mobile. When the person who was called answers their mobile, communication is established.

In the case of an incoming call, the person calling a mobile dials the MSISDN of the requested mobile subscriber. When the call comes from a fixed network subscriber, this conveys the call to the closest MSC, which will act as the GMSC.

The GMSC initiates a procedure close to the HLR of the requested mobile subscriber. The HLR requests a MSRN from the VLR close to which the mobile is recorded and retransmits it to the GMSC. This number is the identity that will allow the call to be transported over the mobile network. The GMSC will be able to establish a circuit with the MSC under the coverage in which the mobile is situated.

The MSC/VLR then broadcasts a paging message containing a TSMI or IMSI in the cells in the location where the requested mobile is situated. The BSC allocates a dedicated SDCCH for signaling exchange. The procedure continues with user authentication, followed by data encryption.

When the subscriber hangs up, all RRs and connections must be released.

1.4.4.2. *Procedures*

1.4.4.2.1. The incoming call

The GMSC requests a temporary MSRN via the MAP SEND ROUTING INFO message to the destination of the HLR. This is relayed to the VLR of the mobile requested by the MAP PROVIDE ROAMING NUMBER message. The message acknowledging the requests allows the GMSC to recover the MSRN (Figure 1.27).

The GMSC can establish a connection with the MSC of the requested mobile via the ISUP initial address message. This provokes the paging procedure within the mobile's location area (Figure 1.27):

– BSSMAP PAGING message to the BSC;

– RR PAGING message by using the PCH on the radio interface.

The network then implements the procedure for the establishment of the dedicated SDCCH, the authentication of the mobile and communication encryption.

On the dedicated SDCCH, the MSC initializes the call via the CM SET UP message and assigns a traffic channel to the mobile via the BSC. The mobile sends the CC ALERTING message to the MSC, which is translated into an ISUP address complete message. When the requested user takes the call, this triggers the transmission of the CM CONNECT message to the MSC which acknowledges the message to the mobile and alerts the GMSC by the ISUP answer message. The connection is achieved and the communication can start (Figure 1.27).

The release of the communication triggers the mobile's transmission of a CM DISCONNECT message to the MSC. This is relayed to the GMSC by the ISUP release message. The GMSC acknowledges this message via an ISUP release complete message. The connections between the MSC and the GMSC are released.

At the same time, the MSC transmits the CM RELEASE message to the mobile, whose acknowledgement triggers the release of the resources at BSS level (Figure 1.27).

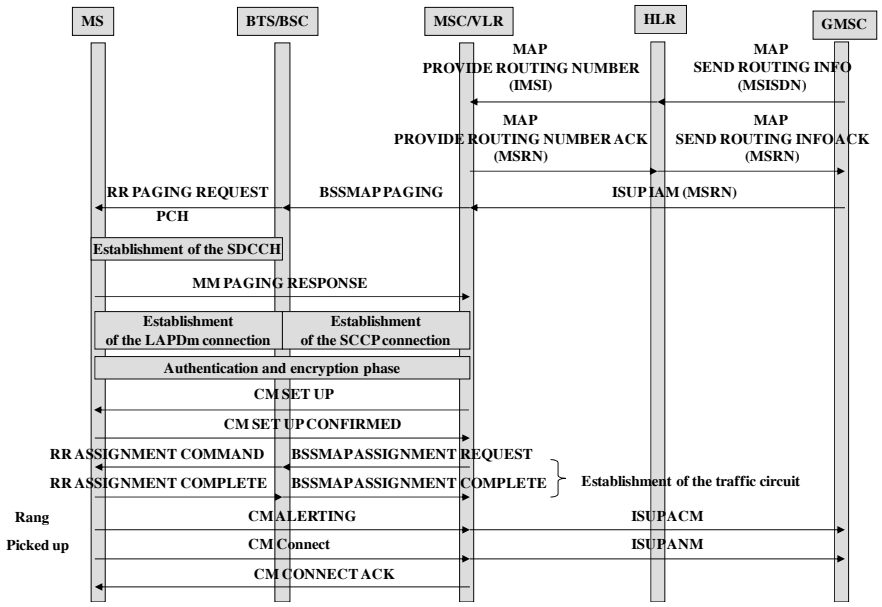


Figure 1.27. *The phases in the establishment of an incoming call*

1.4.4.2.2. The outgoing call

When the mobile initializes an outgoing call, it transmits a CM SERVICE REQUEST message on the RACH. The network then implements the procedure for the establishment of the dedicated SDCCH, mobile and communication encryption authentication (Figure 1.28).

The mobile transmits the number of the user requested in a CM SET UP message, to the MSC, relayed to the TSC via the ISUP initial address message. The mobile receives acknowledgement of its request via the CM CALL PROCEEDING message. The MSC and the BSC then implement the procedure for traffic channel establishment. When the device of the person being called rings, the person calling is notified by the CM alerting message, and the translation of the ISUP address complete message is received by the MSC (Figure 1.28).

When the person called hangs up, the TSC alerts the MSC via the ISUP answer message, which is relayed to the mobile by the CM CONNECT message. After the

mobile acknowledges this message, the connection is established and the call can start (Figure 1.28).

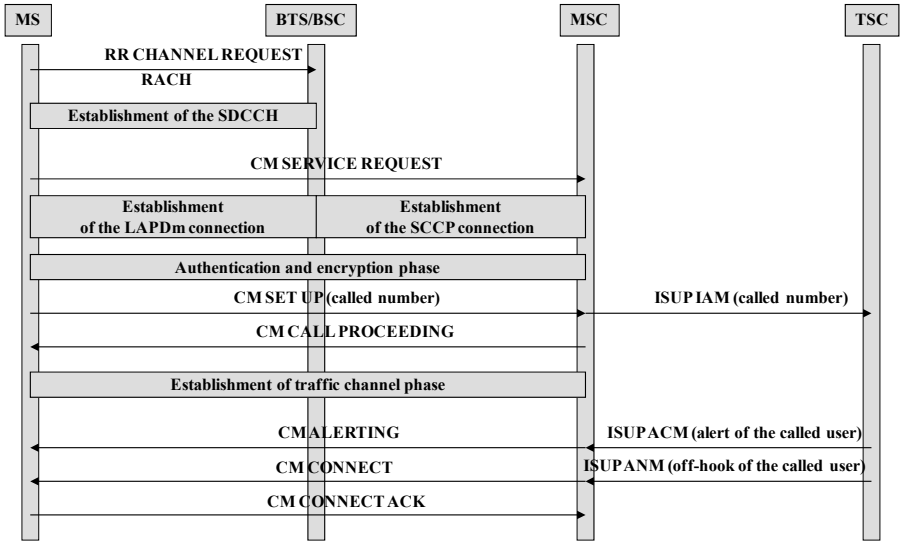


Figure 1.28. *The phases of outgoing call establishment*

1.4.5. *Handover management*

1.4.5.1. *Principals*

The process of cell selection allows a mobile involved in a communication to choose the best cell from the radio link's point of view. The triggering of a cell or handover change is always decided by the network. The handover process is established at the level of the mobile, BSC and MSC.

The handover between two different cells usually happens when the measurements carried out show a weak level of radio field or quality of signal received on the current cell. It is also possible that in order to balance the traffic, the network decides to transfer certain communications to neighboring cells.

When there is a weak level of signal quality received and an elevated level of received field signal, it is likely that deterioration will be linked to interferences and not distance. In this case, the network can make the decision to transfer the communication to another channel.

During a handover procedure, several things may happen, as far as the network is concerned (Figure 1.29):

– the current cell and the new cell depend on the same BSC (intra-BSC handover);

– the current cell and the new cell depend on the same MSC and on two different BSCs (intra-MSC handover);

– the current cell and the new cell depend on two different BSCs and two different MSCs (inter-MSC handover).

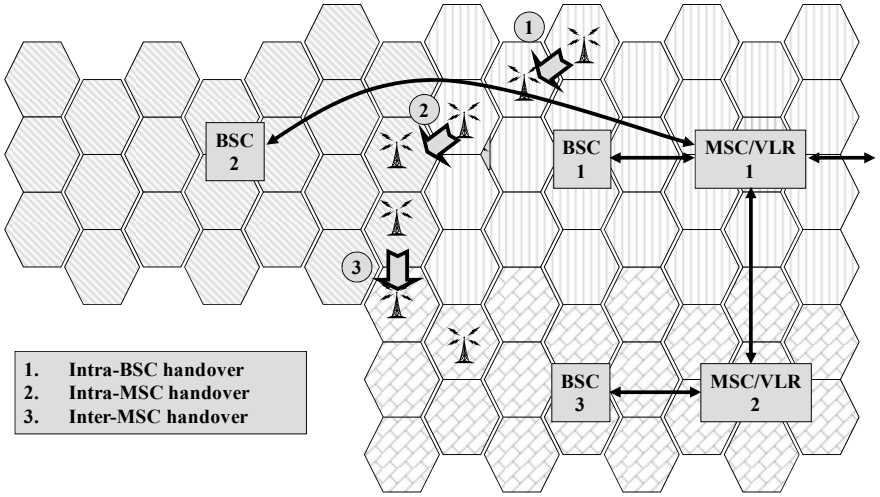


Figure 1.29. *The handover*

1.4.5.2. *Procedures*

1.4.5.2.1. Intra-BSS handover

The BSC uses all the measurements at its disposal to decide on the execution of the handover. The BSC starts to reserve a channel on the new cell by sending a BTSM CHANNEL ACTIVATION message to the new BTS. This activates the channel and acknowledges the request (Figure 1.30).

The BSC then sends a RR HANDOVER COMMAND message to the mobile via the former BTS. This message is transmitted to the FACCH and contains the following information:

– the coordinates of the new dedicated SDCCH and TCH;

– the characteristics of the new cell (frequency of the beacon channel);

– the power level to be used by the MS as the initial power on the new channels;

– the TA to be used in the new cell, if the network can indicate it;

– the eventual establishment of a new mode of encryption.

When the two BTSs concerned in the handover are not synchronized, the BSC cannot know the TA value to be applied to the mobile. The handover is asynchronous.

When the mobile receives the RR HANDOVER COMMAND message, it switches to the channel and cells indicated. It sends the RR HANDOVER ACCESS message on the access burst and not on the normal burst. The new BTS notifies the old BTS via a HANDOVER DETECTION message and calculates the TA to apply to the mobile. It transmits the value to the mobile in a RR PHYSICAL INFORMATION message. The RR HANDOVER ACCESS message is transmitted until the RR PHYSICAL INFORMATION message is correctly received (Figure 1.30).

The mobile can thus establish a connection at frame level on the FACCH. The mobile then sends a RR HANDOVER COMPLETE message, to indicate that the handover was correctly carried out. This message is retransmitted to the BSC. This releases the former channel by sending the BTSM RF CHANNEL RELEASE message to the former BTS, which in turn inactivates the channel and acknowledges the command (Figure 1.30).

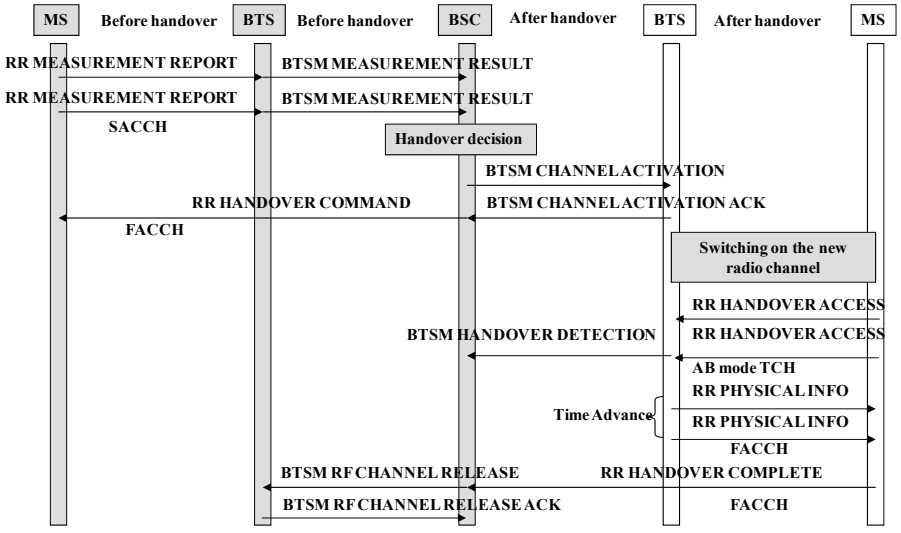


Figure 1.30. *The phases of intra-BSS handover*

1.4.5.2.2. The intra-MSC handover

The original BSC sends a BSSMAP HANDOVER REQUIRED message to the MSC by informing it of the cell to which the mobile must be transferred. The MSC launches the handover procedure by sending the BSSMAP HANDOVER REQUEST message to the destination BSC (Figure 1.31).

When the destination BSC has allocated the resources for the mobile, it sends a BSSMAP HANDOVER REQUEST ACKNOWLEDGE message to the MSC that contains information about the new channel and cell. The MSC relays this message to the mobile via the BSC by transmission of the BSSMAP HANDOVER COMMAND message. This message is relayed by the RR protocol to the mobile (Figure 1.31).

The mobile changes the cell and accesses the dedicated channel as is the case with an intra-BSC handover. The MSC can switch the telephone line upon receipt of the BSSMAP HANDOVER DETECTION message following the mobile's transmission of the RR HANDOVER ACCESS message, without waiting for the handover procedure to finish. The BSC relays the received HANDOVER COMPLETE message from the mobile by using the BSSMAP protocol. The MSC can release all the resources and connections from the former BSS by sending the BSSMAP CLEAR COMMAND message (Figure 1.31).

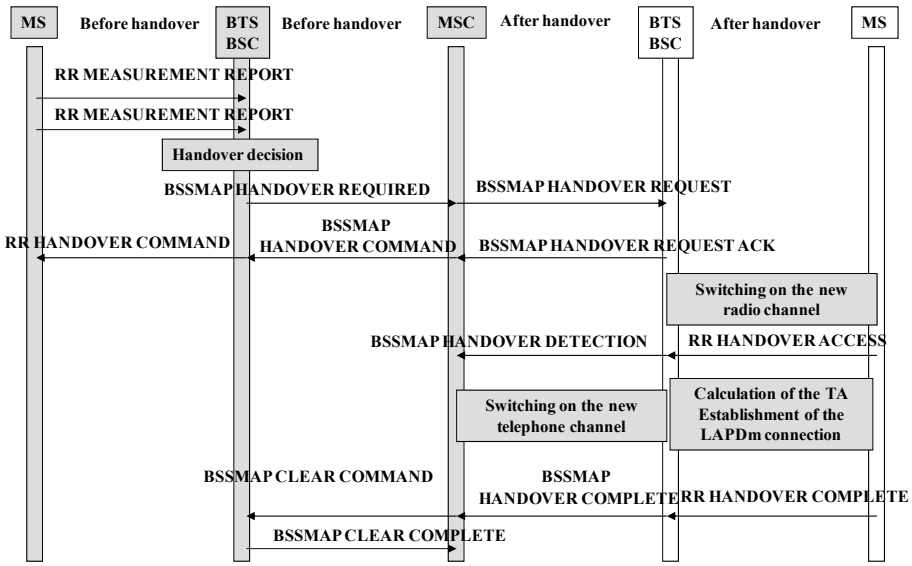


Figure 1.31. *The phases of the intra-MSC handover*

1.4.5.2.3. The inter-MSC handover

When the original MSC receives a handover request from the BSC via the BSSMAP HANDOVER REQUIRED message, it recopies the data from this message and encapsulates it in a MAP PERFORM HANDOVER message, which is sent to the destination MSC. This prepares for connection with the destination BSC, as is the case with the intra-MSC handover (Figure 1.32).

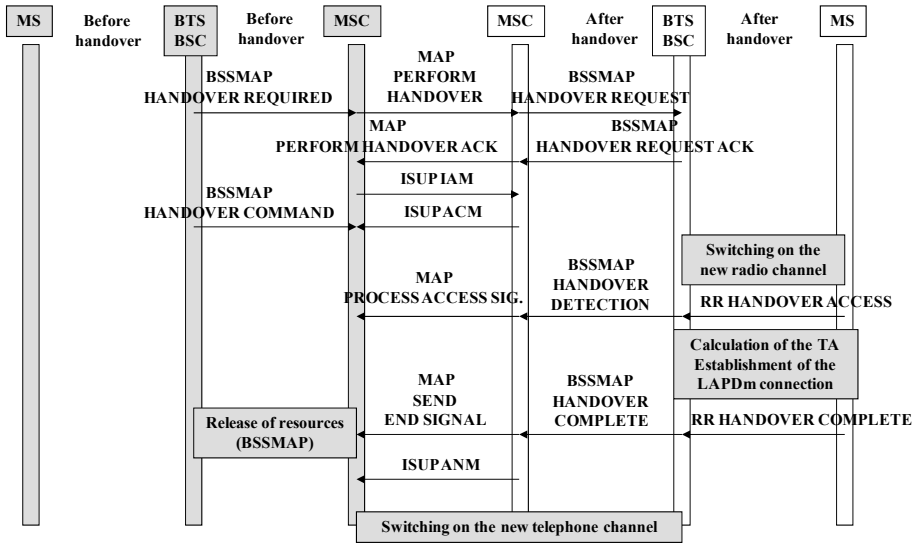


Figure 1.32. *The phases of inter-MSC handover (ANM = ANswer Message; IAM = Initial Address Message)*

If the resources can be reserved on the destination BSS, the MSC/VLR allocates a handover number to the original MSC. This number plays the same role as the MSRN and aims to establish a telephone line, via the ISUP protocol, between the original and the destination MSC.

When a circuit is established between the two MSCs, the original MSC can send the handover command to the mobile. When the mobile is connected to the destination BSS, a HANDOVER DETECTION message is sent to the original MSC, encapsulated in a MAP PROCESS ACCESS SIGNALING message. This message is used to toggle the connection of the original BSS to the destination MSC (Figure 1.32).

When the mobile sends the RR HANDOVER COMPLETE message, this message is retransmitted to the original MSC to notify it that the handover was

carried out correctly and that the resources on the original BSS can be released (Figure 1.32).

The outbound communication stays under the control of the original MSC. When the communication terminates, the original MSC sends a MAP SEND END SIGNAL message in order to release the resources and an ISUP message to release the connection (Figure 1.32).

Chapter 2

The GPRS Network

In this chapter, section 2.1 explains the data transmission service provided by the GPRS (General Packet Radio Service) mobile network. This service is implemented in PS (Packet Service) mode, which has a resource shared by a set of flows reserved for it. The increase in rate at 171.2 kbps is obtained by carrying out a concatenation of the radio channel's eight slots.

Section 2.2 explains the architecture of the GPRS mobile network, which consists of two sub-systems. The BSS (Base Station Sub-system) access network defined within the GSM network is evolving with regard to the method for allocating the radio resource to the mobile. The GSS (GPRS Sub-System) core network is a new entity that is used to establish a link between the BSS networks and the third-party PDN (Packet Data Network) or the Internet.

Section 2.3 describes the radio interface between the mobile and the GPRS mobile network. The description of the transmission chain is essentially concerned with the channel coding, time-division multiplexing of logical channels and the data link protocols.

Section 2.4 describes the procedures concerning the establishment of a session (attachment to the network and detachment), the transfer of traffic, the management of mobile roaming and location management.

Finally, section 2.5 discusses the EDGE (Enhanced Data for Global Evolution), which consists of an increase in the rate to 473.6 kbps thanks to a new type of modulation, for which a new channel coding scheme (CS) is defined.

2.1. Services

The GSM (Global System for Mobile) network is used to implement a data transmission service in circuit mode. This mode monopolizes a radio channel, whatever the activity of the terminal may be. The rate offered by the GSM network is at most 14.4 kbps. The logical channel used is the TCH (Traffic CHannel).

The HSCSD (High Speed Circuit Switched Data) service is a data transmission service in circuit mode that allows a single user to occupy up to four logical TCHs of a radio carrier. The user can have a rate of up to 57.6 kbps. This data service is compatible with a rate of 64 kbps switched by the MSC (Mobile-services Switching Center).

Instead of a radio channel exclusively being used by a user for the entire duration of a communication, the GPRS only allows the radio channel capacity to be acquired when there are data to transmit, thus allowing optimization of radio resources. In optimal propagation conditions, the GPRS is used to attain maximum rates of up to 171.2 kbps, when eight logical TCHs are concatenated (Figure 2.1).

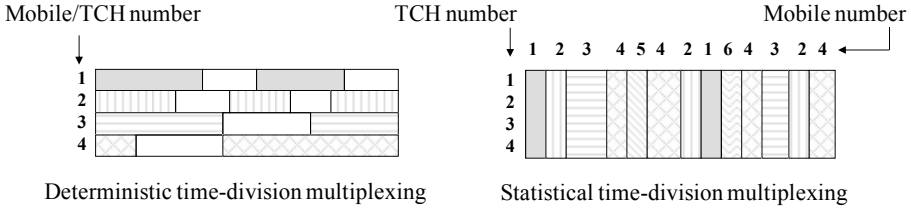


Figure 2.1. *The principles of multiplexing*

Just like the HSCSD, the GPRS requires the introduction of new mobile phones. Contrary to the HSCSD, however, the GPRS requires the establishment of new elements in the BSS and the introduction of a GSS for packet routing.

The GPRS network has four rate classes (CS1, CS2, CS3 and CS4). Each rate class corresponds to a different CCU (Channel Codec Unit), which is implemented at BTS (Base Transceiver Station) and mobile level (Table 2.1).

The services offered by the GPRS network are characterized by quality of service. This includes several criteria, such as the loss ratio or delay (Tables 2.2 and 2.3). Three classes of service are offered. They allow the operator to manage the network congestion situation by diverting the least urgent traffic.

Service	Channel coding	Rate by slot	Maximum rate
HSCSD	TCH/14.4	14.4 kbps	4*14.4 kbps = 57.6 kbps
GPRS	CS1	9.05 kbps	8*9.05 kbps = 72.4 kbps
	CS2	13.4 kbps	8*13.4 kbps = 107.2 kbps
	CS3	15.6 kbps	8*15.6 kbps = 124.8 kbps
	CS4	21.4 kbps	8*21.4 kbps = 171.2 kbps

Table 2.1. *Rate classes*

The levels of loss ratio correspond to different guarantees on the probability of loss, duplication and data sequencing.

Different classes of delay are also defined with regard to packet size.

Class 4 (best effort) provides no service guarantee on these criteria.

Class	Probability of loss	Probability of duplication	Probability of desequencing
1	10^{-9}	10^{-9}	10^{-9}
2	10^{-4}	10^{-5}	10^{-6}
3	10^{-2}	10^{-5}	10^{-2}

Table 2.2. *Service classes – rate loss*

Class	128 bytes		1,024 bytes	
	Average delay	95% delay	Average delay	95% delay
1	< 0.5 s	<1.5 s	<2 s	<7 s
2	<5 s	<25 s	<15 s	<75 s
3	<50 s	<250 s	<75 s	<375 s

Table 2.3. *Service classes – delay*

2.2. Network architecture

2.2.1. *Network components*

2.2.1.1. *The infrastructure network*

The introduction of the GPRS is not a large upgrade on the existing GSM network's infrastructure. The impact essentially concerns the addition of new entities in the network (Figure 2.2):

– the SGSN (Service GPRS Support Node) and the GGSN (Gateway GPRS Support Node), which constitute the GSS network and ensure packet routing;

– the PCU (Packet Control Unit) function introduced into the BSS, which ensures allocation of the radio resource to the mobile and interface with the SGSN.

The SGSN ensures the packet routing functions between the BSS, the GGSN and user management (roaming and mobility management). The GGSN ensures the packet routing to the external data networks (for example the Internet network).

Location management is ensured by the HLR (Home Location Register) as it is for a GSM network in circuit mode. It contains information regarding the correspondence between the IMSI (International Mobile Subscriber Identity) identifier and the PDP (Packet Data Protocol) context of the user. The PDP context contains the different attributes of the user (for example their Internet Protocol or IP address).

The interconnection between the BSS and the SGSN is provided by a frame relay data network, offering a maximum rate of 2 Mbps. The interconnection between the SGSN and the GGSN is provided by an IP data network.

The GSS is connected to different entities deployed for the GSM network (BSS, MSC and HLR) and to exterior networks via the following interfaces:

– the Gb interface, between the BSS (PCU function) and the SGSN, using the Frame Relay protocol;

– the Gr interface, between the SGSN and the HLR, using an extension of the MAP (Mobile Application Part) protocol;

– the Gs interface, between the SGSN and the MSC, using an extension of the BSSMAP (BSS Management Application Part) protocol, for operations shared by the GSM and the GPRS;

– the Gd interface, between the SGSN and the SMSC, using an extension of the MAP protocol, for sending SMS (Short Message Service) messages via the GPRS network;

– the Gc interface between the GGSN and the HLR, using an extension of the MAP protocol;

– the Gi interface, between the GGSN and the data networks, using the IP.

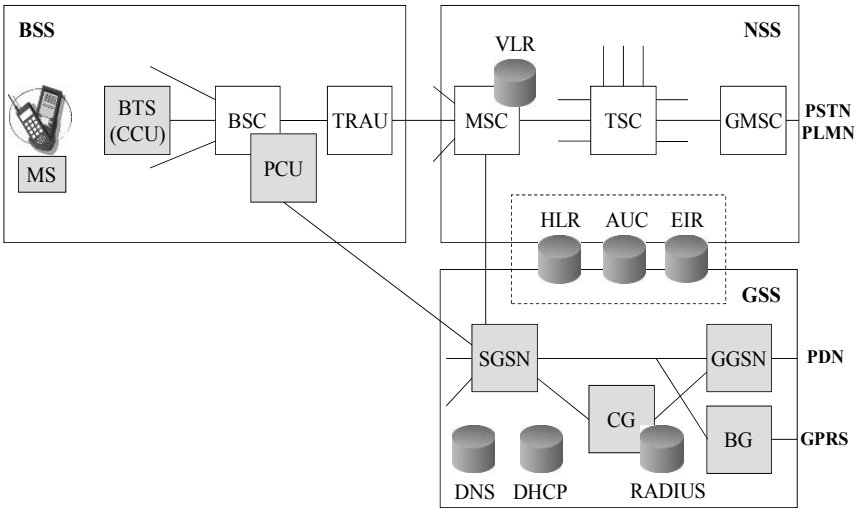


Figure 2.2. *The architecture of the network*

The interconnection between the GGSN and the SGSN is carried out via the Gn interface. Data routing uses a GTP (GPRS Tunnel Protocol) on this interface. The tunnel mode consists of placing the user's data (for example an IP packet) in another protocol data unit (IP) without the latter concerning itself with the format of the transported data.

When the user starts a GPRS session, in its request it specifies the APN (Access Point Name) address of the access point to the external network in the form of a character string. The SGSN queries the DNS (Domain Name Service) in order to determine the IP address of the GGSN concerned.

The IP address of the user is dynamically allocated by a DHCP (Dynamic Host Configuration Protocol) server. In the case of an allocation of addresses in transparent mode, the IP address is managed by the operator of the GPRS network. In the case of an allocation of addresses in non-transparent mode, the IP address is managed by an external server.

The charging gateway entity collects the billing tickets from the SGSN and GGSN and ensures the interface with the RADIUS (Remote Authentication Dial In

User Service) server. The RADIUS server is used to issue traffic authorizations (for example the volume of data transferred) and to carry out the logging and billing of traffic.

The border gateway entity ensures a function equivalent to the GGSN. It is used during the interconnection between two GPRS networks, when the mobile is on a visitor network.

2.2.1.2. *The mobile*

Three classes of mobile are defined according to their capacity to simultaneously use the GSM network (speech in circuit mode) and the GPRS network (data in packet mode):

– a class A mobile can simultaneously use the services offered by the GPRS and GSM networks;

– a class B mobile can sequentially use the services offered by the GSM or GPRS networks;

– a class C mobile can use the services offered by the GPRS network or the GSM network. It is different from the class B mobile in the sense that it does not have a standby mode that scans both types of network.

The number of slots used for the uplink and downlink radio channel refers to one in 29 mobile classes. Class 1 uses one slot for each radio channel. Class 29 uses eight slots for each radio channel.

Type 1 mobiles (classes 1 to 12 and 19 to 29) function in half-duplex. The transmission and reception are carried out at different distances. Type 2 mobiles (classes 13 to 18) function in full duplex, and the transmission and reception are carried out simultaneously.

2.2.2. *Protocol architecture*

2.2.2.1. *The traffic plan*

The traffic plan comprises all protocol layers used to send data between the mobile and the service platforms. In order to have a communication channel, a data link is established using the LLC (Logical Link Control) protocol between the mobile, the SGSN and a GTP tunnel for exchanges between the SGSN and the GGSN (Figure 2.3).

The LLC protocol functions either in unacknowledged mode, by not concerning itself with packet losses, or in acknowledged mode by applying retransmissions and

flow control in order to ensure that the data are correctly supplied. It also takes charge of link encryption and ensures signaling transfer.

The GTP relies on the transport protocols TCP (Transport Control Protocol) and UDP (User Datagram Protocol). The TCP provides flow control and protection against GTP data unit loss. The UDP is used for unreliable transport between the SGSN and GGSN.

The SGSN and GGSN are connected to a data network based on the IP. The GTP data units, encapsulated in TCP or UDP transport units, are then encapsulated by an IP header. This IP network is concerned solely with delivery between the SGSN and GGSN.

The purpose of the SNDCP (Sub-Network Dependent Convergence Protocol) convergence layer is to reuse standard protocols of IP-fixed networks by having a single lower LLC layer. It carries out the compression of TCP/IP headers and traffic data, as well as IP data unit segmentation.

The RLC (Radio Link Control) protocol provides a data link with a flow control mechanism for traffic and signaling between the mobile and the BSC (Base Station Controller). It relies on a MAC (Medium Access Control) layer that controls access to the radio channel and puts the LLC frames and logical channels in contact with one another.

The BSS GPRS Protocol is similar to the BSSMAP protocol. It manages traffic between the BSS and the SGSN.

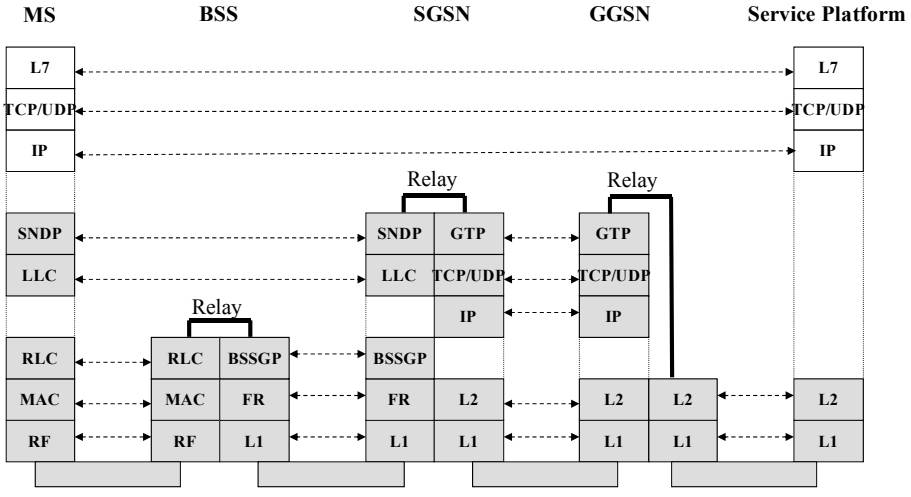


Figure 2.3. *The protocol architecture – the traffic plan*

2.2.2.2. *The signaling plan*

The signaling plan consists of a set of protocol layers that are used to achieve the following functions (Figure 2.4):

– control of access to the GPRS network with the GPRS Attach and GPRS Detach procedures;

– control of the attributes linked to a session, such as the activation of a PDP context;

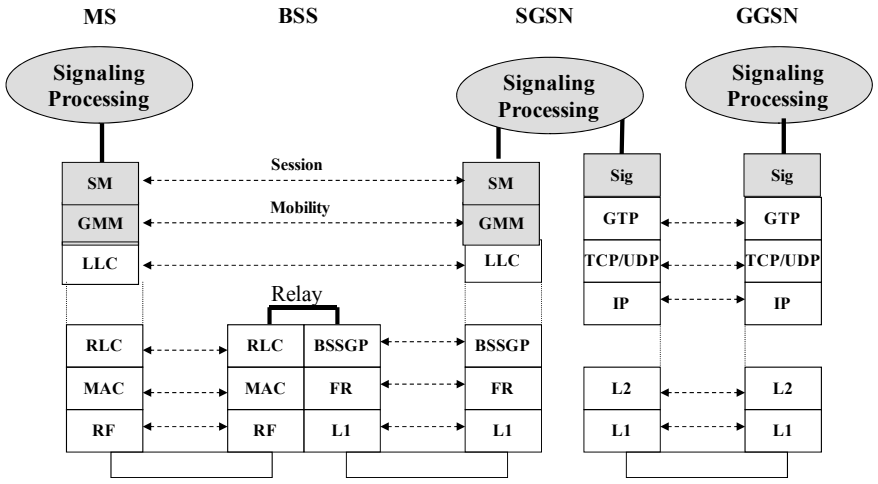
– updating of routing information to support roaming;

– dynamic allocation of network resources according to user requests.

The SS7 (Signaling System 7) signaling stack that bears the MAP protocol for the GSM is reused in the SGSN for connection to the HLR via the Gr interface and to the equipment identity register via the Gf interface.

The GTP tunnel is reused in the signaling plan between the SGSN and the GGSN as in the traffic plan, by relying on the transport UDP.

At the level of the Gs interface, between a SGSN and a MSC, signaling procedures have been added to the BSSMAP protocol for roaming management.



FR – Frame Relay
L1 – Layer 1
L2 – Layer 2
Sig – Signaling

Figure 2.4. *Protocol architecture – the signaling plan*

The signaling protocols are exchanged between the SGSN and the mobile relay on the same layers used in the traffic plan (Figure 2.4):

– the GMM (GPRS Mobility Management) protocol designates all functions that deal with mobility;

– the SM (Session Management) protocol designates all functions linked with SM.

2.2.3. *Logical identifiers*

Logical identifiers are implemented at certain layers in order to identify whether the packet belongs to a user or to a user's session.

Between the BSC and the different mobiles, the data flows exchanged can use the same physical resource. Each flow is located in the RLC layer by a TFI (Temporary Flow Identifier), see Figure 2.5.

The GPRS network can allocate a temporary P-TMSI (Packet Temporary Mobile Subscriber Identity), which is similar to the TMSI, to a mobile. The (class A or class B) mobile is therefore seen to allocate two identities: the TMSI for the GSM traffic and the P-TMSI for the GPRS traffic.

The link between the BSC and the GGSN at Gb interface level transports several flows of different users on the same logical frame relay connection, which is located by a TLLI (Temporary Link Layer Identity) identifier located at the BSS GPRS protocol layer (Figure 2.5).

If the mobile has a P-TMSI, the TLLI is identical to it. When the mobile must gain access without having a P-TMSI, it uses a random TLLI, which will be replaced as soon as possible by the P-TMSI. When the mobile that has a P-TMSI changes SGSN, there can be conflict between two mobiles using the same TLLI. To avoid this, the mobile uses a foreign TLLI derived from the P-TMSI, by changing the two most significant bits.

Each link between the mobile and the SGSN is carried by the LLC layer. This link consists of signaling messages, text messages corresponding to the SMS and traffic messages. The different types of messages are located in the LLC layer by the SAPI (Service Access Point Identifier), see Figure 2.5.

The SNDCP layer contains the user's different traffic flows. Each one corresponds to an access point in the external network. Each flow type is located by a NSAPI (Network Service Access Point Identifier), see Figure 2.5.

The user can open several sessions with different service qualities on the same terminal. The PDP context must be created so that the user can transmit and receive

data from each external network. A different type of PDP context is stored in the mobile, the SGSN and the GGSN.

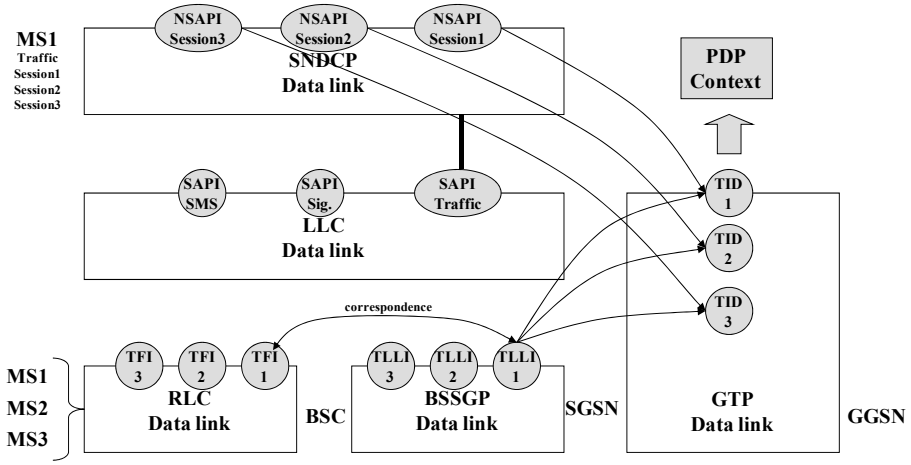


Figure 2.5. *Logical identifiers*

A PDP context contains the type of network used, the mobile's PDP address (IP address), the IP address of the SGSN on which the mobile is situated, the APN for the exterior network and other parameters, such as the quality of service or the logical identifiers.

A mobile can simultaneously activate several sessions identified by the NSAPI. The mobile is identified close to the SGSN by the TLLI. The (TLLI/NSAPI) couple clearly identifies a PDP context for the link between the SGSN and the mobile. The TID (Tunnel) identifier identifies the PDP context for the link between the SGSN and the GGSN.

2.2.4. *Mobility context*

Mobility environment contains the parameters linked to mobility management, such as the user's identities (IMSI and P-TMSI) and the mobility state of the mobile (IDLE, STANDBY or READY).

In the GSM network, the mobile can be in two states: on or off. When it is on, the location area where it is situated is memorized in the HLR, whether it is in a communication or on standby. The state is managed by the IMSI Attach and IMSI Detach procedures.

In the GPRS network, the mobile can have three states:

– the IDLE state, corresponding to a mobile that is switched or logged off;

– the STANDBY state, corresponding to a mobile located in the routing area;

– the READY state, corresponding to a mobile located in the nearby cell.

Two machines function in parallel in the mobile and the SGSN. These machines highlight the different functions necessary to change the state (Figure 2.6).

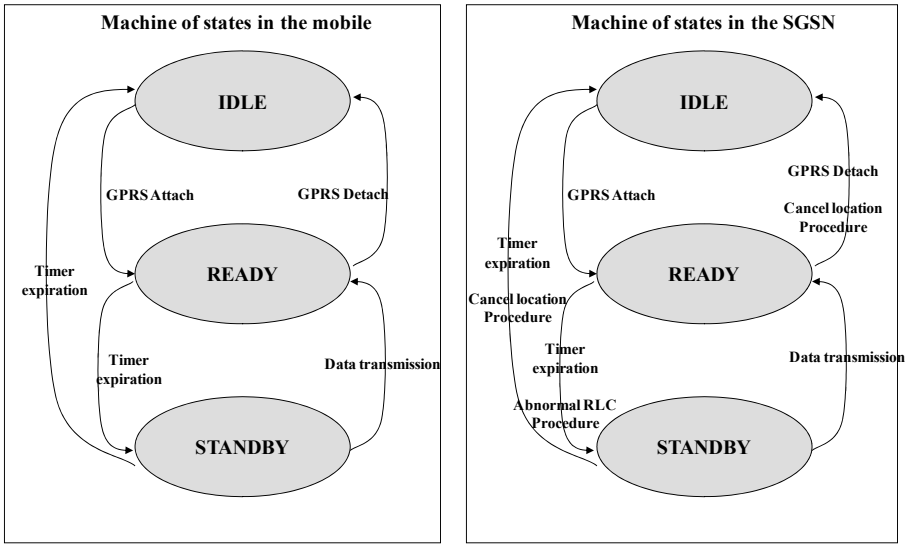


Figure 2.6. *The mobility management machines*

A mobile in IDLE state that connects to the GPRS network, via the GPRS Attach procedure, switches to the READY state. It returns to the IDLE state if it disconnects from the GPRS network via the GPRS Detach procedure. From the READY state, the mobile switches to the STANDBY state if it does not have data to transmit at the end of a timeout.

Transition to the STANDBY state allows for the release of radio and network resources for signal processing. It returns to the READY state during a data transmission. From the STANDBY state, the mobile can switch to the IDLE state at the end of a timeout.

The functioning of the machine in the SGSN reveals additional functions that cause a change in state. From the READY state, the mobile can switch to

STANDBY if it is forced by the SGSN or if there is an error (Abnormal RLC Procedure). From the STANDBY or the READY state, the mobile terminal can switch to the IDLE state during the Cancel Location procedure.

2.2.5. *The WAP gateway*

Mobile terminals have a more limited environment than desktop computers: they have less powerful processors, less memory capacity and smaller screens.

Moreover, mobile networks have a more constrained environment compared to fixed networks, with reduced bandwidth, longer delay and unpredictable availability.

The WAP (Wireless Application Protocol) model is used to optimize and improve the use of the TCP/IP model in a mobile network by providing the following functions:

– a gateway translating the TCP/IP stack into a new WAP stack;

– a compression device for the transmitted data;

– terminal profile management to adapt the data to the capabilities of the terminal.

The WAP terminal communicates with the WAP proxy (or gateway) connected to the GPRS mobile network, and more precisely at GGSN level. The WAP proxy translates the WAP requests into HTTP (HyperText Transfer Protocol) requests, thus allowing the WAP client to access a Web-server.

If the Web-server proposes a WAP content, for example, by using the WML (Wireless Markup Language) syntax, the WAP proxy directly recovers content from the Web-server. If the Web-server proposes content with the HTML (HyperText Markup Language) syntax, a filter is used to translate it into WAP content.

2.2.5.1. *The 1.x WAP gateway*

The 1.x WAP gateway translates the TCP, TLS (Transport Layer Security) protocol and HTTP of the Internet model (Figure 2.7).

The WAE (Wireless Application Environment) protocol is an application environment whose objective is to establish an interoperable environment that will allow the operators and service providers to construct applications. WAE includes a micro-browser environment in the mobile containing the following functions:

– a lightweight WML, similar to HTML but optimized for the use of mobile terminals;

– a WML lightweight script language, similar to JavaScript™;

– a group of data formats.

The WSP (Wireless Session Protocol) provides the application layer with an interface for two types of session:

– the first is a connection-oriented service that functions above the WTP (Wireless Transaction Protocol). This is adapted to the navigation on WAP sites;

– the second is a connectionless service that functions above the WDP (Wireless Datagram Protocol). This is used for information that is spontaneously sent (push mode).

The WTP provides the session layer. It is used for three types of request:

– the sending of unacknowledged unidirectional requests;

– the sending of acknowledged unidirectional requests;

– the sending of acknowledged bidirectional requests.

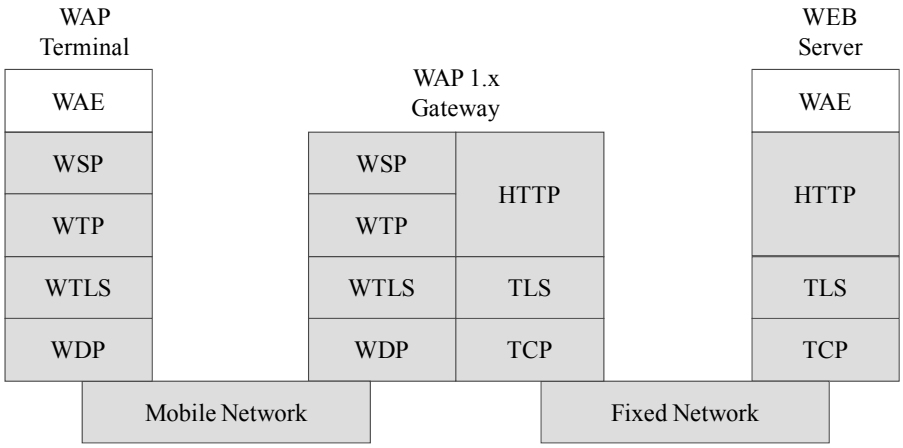


Figure 2.7. *The 1.x WAP gateway*

The WTLS (Wireless Transport Layer Security) protocol is a security protocol based on the TLS protocol. It provides the authentication, integrity and privacy functions for data. It authorizes a dynamic refresh of the secret key during the transaction without going via the renegotiation phase.

The WDP provides a transport layer equivalent to the UDP. It ensures independence via the mobile data network. It is used for addressing ports

corresponding to applications and, optionally, the segmentation and reassembly of the segments as well as error detection.

2.2.5.2. *The 2.0 WAP gateway*

The 2.0 WAP gateway introduces Internet protocols into the WAP environment, following the increase in the rate of the mobile network radio interface.

The 2.0 WAP model specifies the profile used for the TCP and HTTP. Several cases can arise:

– The 2.0 WAP gateway does not modify the profiles. In this instance it carries out a simple IP routing (Figure 2.8).

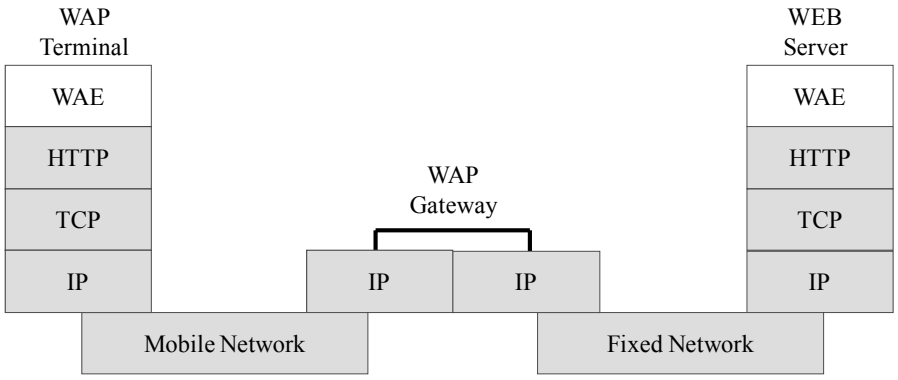


Figure 2.8. *The WAP 2.0 gateway – IP routing*

– The 2.0 WAP gateway uses the TCP WP (Wireless Profile) on the mobile network. In this instance it carries out a TCP relay (Figure 2.9).

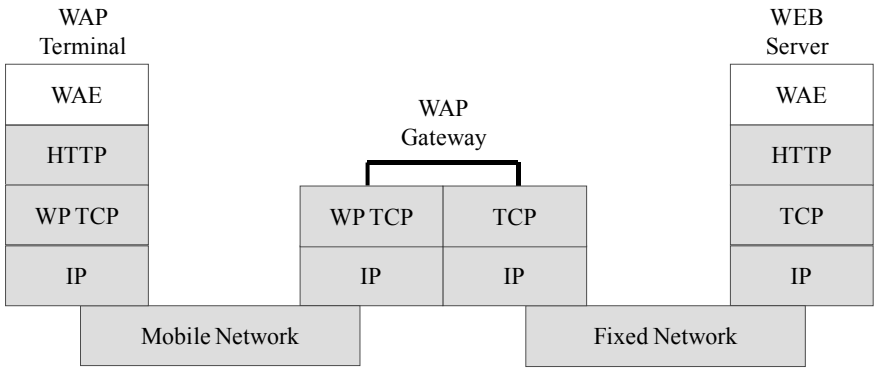


Figure 2.9. *The WAP 2.0 gateway – TCP relay*

– The 2.0 WAP gateway uses the WP TCP and WP HTTP profiles on the mobile network. In this instance it executes an HTTP gateway (Figure 2.10).

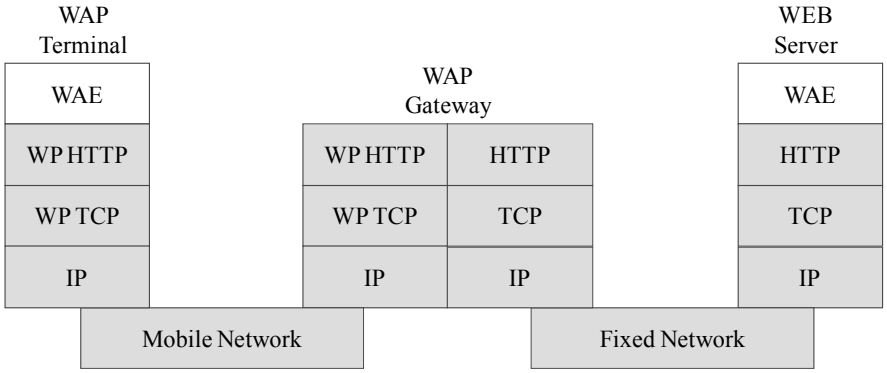


Figure 2.10. *The WAP 2.0 gateway – HTTP gateway*

2.2.6. *Roaming between operators*

It is possible that two GPRS mobile operators can link straight up to one another. However, this tendency cannot be generalized to all those in operation, because each operator will deploy hundreds of links.

The GRX (GPRS Roaming eXchange) network is an IP transit network that ensures the interconnection of GPRS mobile networks in order to ensure that roaming between operators in possible (Figure 2.11).

The GRX providers must be able to request that mobile operators exchange flow not only with mobile operators, who are directly linked up to their network, but also with all mobile operators who pass through other GRX operators. The GRX providers connect to each other and the exchanges are made by means of peering points.

The SGSN of the visited mobile networks receives the (APN) request from the mobile. It sends this address resolution request to its DNS, which might not be able to determine the address.

The DNS of the visited network thus contacts the root DNS, which responds to this request by giving the IP address of the domestic network DNS. It then contacts the DNS of the domestic network, which resends the GGSN's IP address.

Once the IP address of the GGSN has been determined, an IP tunnel is formed between the SGSN of the network being visited and the GGSN of the home

network. From the latter, the subscriber can access their sessions as if they were on the home network.

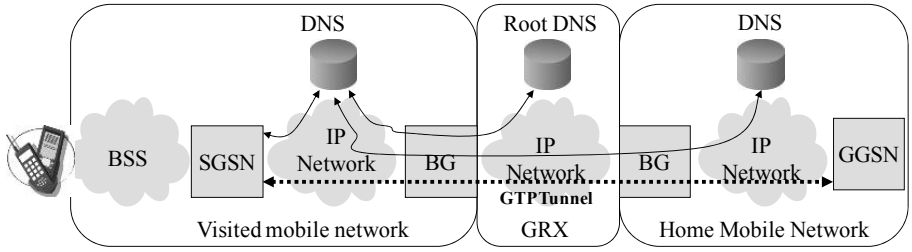


Figure 2.11. *Roaming between operators*

2.3. Radio interface

2.3.1. *The transmission chain*

The user's data (IP packet and signaling messages) are subject to different types of processing: on the one hand at mobile level and on the other hand at BTS, BSC (PCU function) and SGSN level (Figure 2.12).

The SNDCP protocol is exchanged between the mobile and the SGSN. It can carry out the multiplexing of several data units, their compression and segmentation. It provides the access point to the NSAPI service that identifies the user's sessions (traffic data).

The LLC protocol is exchanged between the mobile and the SGSN. The protocol carries out the data transfer with or without acknowledgement and data encryption. It provides the access point to the SAPI service, which identifies the type of data (signaling, SMS or traffic).

The RLC and MAC protocols are exchanged between the mobile and the BSC (PCU function). The RLC protocol segments the LLC frames into small blocks that are compatible with transmission on the radio interface and reassembles them. It also carries out error control, with selective retransmission of the erroneous block. The MAC protocol allows several mobiles to dynamically share a common radio resource.

Regarding the GSM, the physical layer of the radio interface defines new mechanisms for channel coding and time-division multiplexing. It preserves the same interleaving principal and the GMSK (Gaussian Minimum-Shift Keying)

modulation type. The encryption is no longer achieved at the level of the physical layer; it is transferred to the level of the LLC layer.

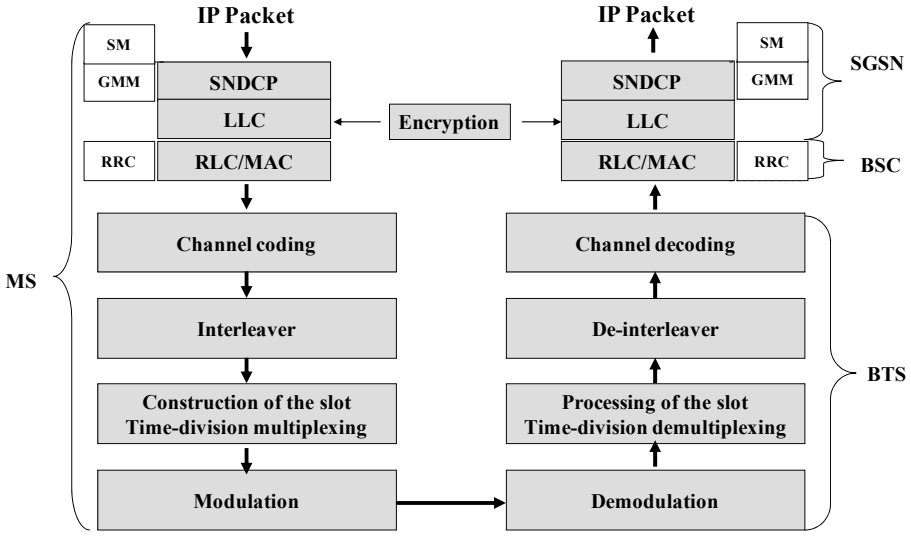


Figure 2.12. *The transmission chain*

2.3.2. *The MS–BSS interface*

2.3.2.1. *Physical layer*

The CCU function is in charge of the transmission functions between the mobile and the BTS. The difference with regard to the GSM resides in the type of channel coding, the structure of the multi-frame and the construction of the logical channels.

The CS type of coding is either defined in a fixed manner, or dynamically by the PCU function, according to the quality measured on the radio link.

For the CS1 type of coding, 40 bits of BCS (Block Check Sequence) redundancy check are added to 181 bits of data from the RLC/MAC layer and to 3 bits of the USF (Uplink State Flag) field to form a block of 224 bits. This block will be completed by 4 trail bits and a convolutional code is applied to the totality to obtain a block of 456 bits (Figure 2.13).

For the CS2 type of coding, the 3 bits of the USF field are protected because the data are less well protected. A BCS field of 16 bits for the redundancy check is added to the 268 bits of data from the RLC/MAC layer and to the 6 bits of the USF

field in order to obtain a 290-bit data block. This block will be completed by the addition of 4 trail bits and a convolutional code will be applied to this in order to obtain a block of 588 bits. The puncturing operation consists of removing 132 bits from 588-bit block, with the exception of the USF field, in order to obtain a block of 456 bits (Figure 2.13).

For the CS3 type of coding, the 3 bits of the USF field are protected in a way that is identical to CS2 coding. CS3 coding added to 312 bits of data from the RLC/MAC layer and to 6 bits of the USF field, a BCS field of 16 bits for the redundancy check in order to obtain a data block of 334 bits. This block will be completed by the addition of 4 trail bits and a convolutional code will be applied to the totality in order to obtain a block of 676 bits. The puncturing operation consists in removing 220 bits from the 588-bit block, with the exception of the USF field, in order to obtain a block of 456 bits (Figure 2.13).

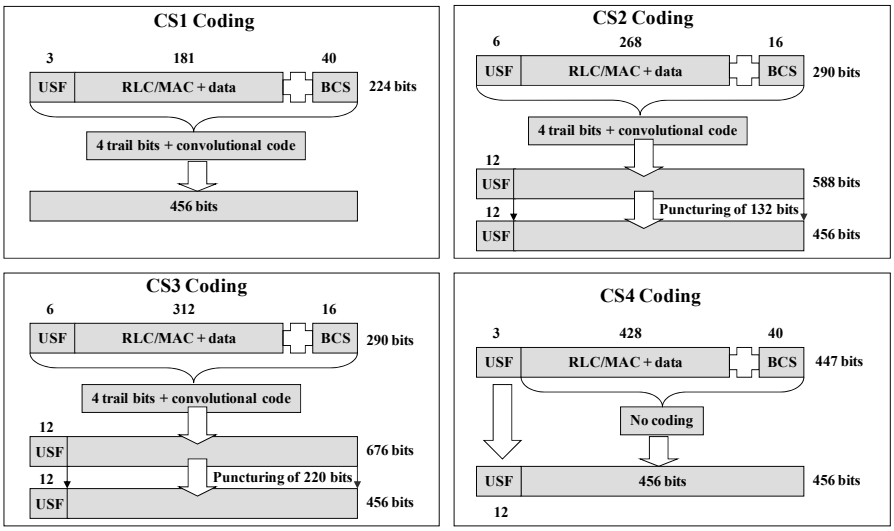


Figure 2.13. *Channel coding*

For the CS4 coding type, the 3 bits of the USF field and the 428 bits of data from the RLC /MAC layer are added to the BCS 16 bits of redundancy check to obtain a block of 447 bits. The USF field is protected by 9 additional bits (Figure 2.13).

The block of 456 bits then sustains the same interleaving process as the GSM, to obtain eight demi-bursts of 57 bits. The structure of the normal burst remains identical to that of the GSM. The preemption bits, which allow the GSM to

differentiate the logical TCH and FACCH (Fast Associated Control CHannel), are used to indicate the type of coding.

The structure of the multi-frame consists of 52 slots, divided into 12 blocks of four slots, with two slots assigned to the PTCCH logical channel and two idle slots (Figure 2.14).

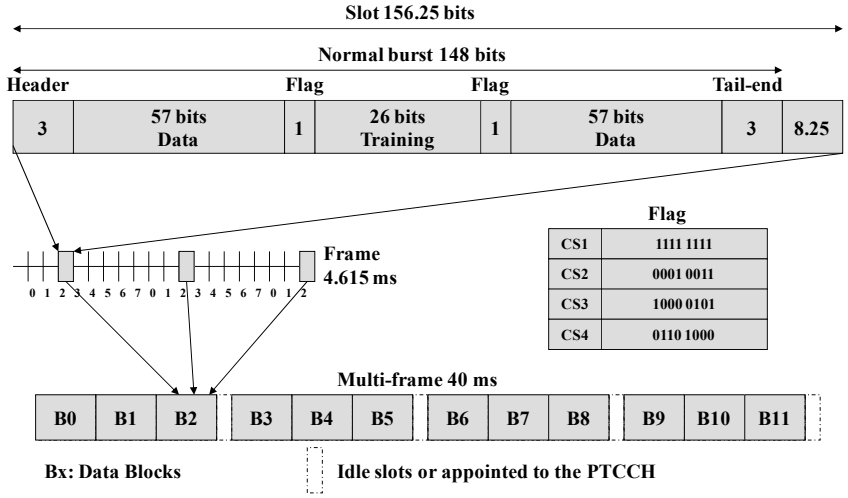


Figure 2.14. *The structure of the bust and multi-frame*

The use of these blocks by logical channels is not fixed, as is the case with the GSM. It can be variable and in the following order: B0, B6, B3, B9, B1, B7, B4, B10, B8, B5, B11. The use of blocks is indicated in the System Information 13 communicated by the BCCH (Broadcast Control CHannel) logical channel of the GSM.

The idle slot is used by the mobile for synchronization on the logical FCCH (Frequency Correction CHannel) in order to decode the SCH (Synchronization CHannel) and measure the signal of neighboring cells.

The GPRS network uses the logical channels of the GSM: FCCH for frequency synchronization, SCH for slot synchronization and BCCH for system information. The other logical channels are classed into three families:

– PCCCH (Packet Common Control CHannel), for common control;

– PBCCH (Packet Broadcast Control CHannel), for the broadcasting of system information;

– PDCH (Packet Data CHannel), for dedicated traffic and control channels.

Table 2.4 contains the list of the GPRS logical channels.

Category	Name	Direction
Broadcasting	PBCCH (*Packet Broadcast Control CHannel*)	Downlink
Common control	PAGCH (*Packet Access Grant CHannel*)	Downlink
Common control	PPCH (*Packet Paging CHannel*)	Downlink
Common control	PRACH (*Packet Random Access CHannel*)	Uplink
Common control	PNCH (*Packet Notification CHannel*)	Downlink
Dedicated control	PACCH (*Packet Associated Control CHannel*)	Bidirectional
Dedicated control	PTCCH (*Packet Timing Control CHannel*)	Bidirectional
Dedicated traffic	PDTCH (*Packet Data Traffic CHannel*)	Bidirectional

Table 2.4. *The GPRS logical channels*

Certain GSM logical channels can replace those corresponding to the GPRS. The logical BCCH broadcasts the System Information 13 message indicating whether the PBCCH is present in the cell. When the PBCCH is absent, the System Information 13 message gives the following information:

– the RAI (Routing Area Identity);

– the parameters of network control;

– the options available on the cell;

– the parameters of power control.

The dedicated logical PDTCH of the GPRS differs from the logical TCH of the GSM on the following two points:

– the PDTCH can be allocated either for downlink or for uplink when functioning in half-duplex;

– the logical PACCH can be transmitted in any of the slots of the uplink channel, and because of this fact preempt the position of the PDTCH.

In a same multi-frame comprising 12 blocks assigned to the PDCH, it is possible to allocate up to eight blocks for one user or to allocate the blocks to eight different users. Allocation of these blocks is managed by the RLC/MAC layer, which assigns the blocks to different users either statically or dynamically.

The PACCH transports the signaling dedicated to a user and corresponds to the SDCCH (stand-alone dedicated control channel), SACCH (slow associated control channel) and FACCH of the GSM.

The PTCCH transports an access burst onto the uplink channel allowing the BTS to calculate the value of the TA (time advance), and on the downlink, the value of the TA to apply to the mobile.

When the mobile wants to transmit data, beforehand it must send a resource request on the access PRACH if this GPRS logical channel is configured in the cell or on the RACH (Random Access CHannel) if the PRACH is not implemented.

The PCU function resends a message containing two identifiers assigned to the mobile (USF and TFI). This message is on the logical PAGCH if this channel is configured in the cell or on the AGCH (Access Grant CHannel) if the PAGCH is not implemented.

The PCU function can alert the mobile in the event of an incoming call by broadcasting a paging message containing the P-TMSI on a PPCH when this channel is configured in the cell or on the AGCH if the PAGCH is not implemented.

The PNCH (Packet Notification CHannel) is used to send notification to a group of users in the case of a point-to-multipoint data transmission.

2.3.2.2. *The RLC/MAC layer*

The RLC/MAC layer is shared by traffic and control data. It consists of an encapsulation of the data derived from the LLC layer. The RLC/MAC layer provides a block of data to the physical layer to create four bursts. The control blocks can contain messages regarding resource allocation or protocol acknowledgement. The structure of the header is specific for each direction of transmission.

2.3.2.2.1. Traffic data

The MAC sub-layer's purpose is to define the rules of resource sharing between mobiles. It consists of the following fields for the downlink (Table 2.5):

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
PT		RRBP		S/P	USF		

Table 2.5. *The structure of the MAC header – downlink*

– USF: this field is used to indicate a dynamic allocation from the uplink channel to each mobile. The contents of the downlink block are decorrelated from the USF and can be allocated to another mobile (Figure 2.15).

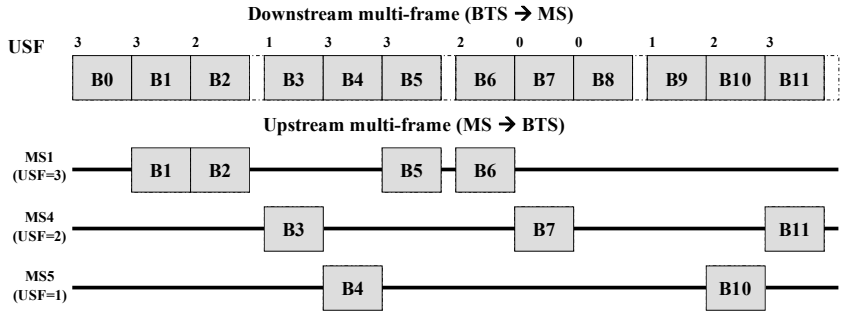


Figure 2.15. *Sharing of the uplink by USF*

– PC (Polling Control): this field is used for the query mechanism. It includes a S/P (Supplementary Polling) query indicator that reserves one of the uplink blocks following the mobile that the downlink block is intended for. It also includes a RRBP (Relative Reserve Block Period) counter that specifies the position of the block concerned (Figure 2.16).

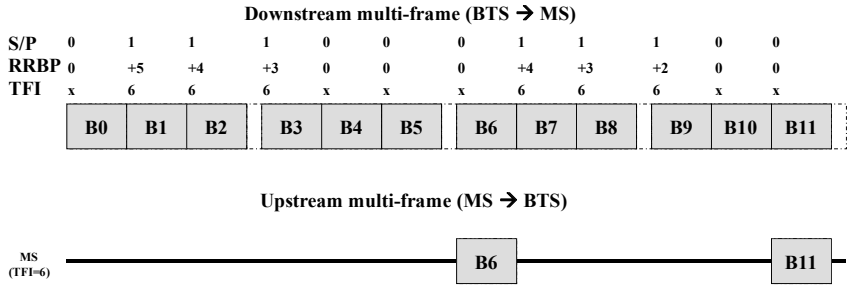


Figure 2.16. *Mobile query*

– PT (Payload Type): this field is used to identify the nature of the LLC data, to determine whether it is a traffic block or a control block.

The MAC sub-layer consists of the following fields for the uplink (Table 2.6):

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
PT		CV				SI	R

Table 2.6. *The structure of the MAC header – uplink*

– R (Retry): this bit indicates whether one or several request messages have been transmitted by the mobile during the access procedure.

– SI (Stall Indicator): this bit indicates whether the mobile's transmission window is full or not.

– CV (Countdown Value): this field is used in the uplink to indicate to the network the number of blocks that are left to transmit. This indication allows the network to manage uplink sharing between different mobiles.

The RLC sub-layer allows for the transport of LLC data units between the mobile and the BSC. It consists of the following fields for the downlink (Table 2.7):

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
PR		TFI					FBI
BSN							E
LI						M	E
LLC data unit							
LI						M	E
LLC data unit							

Table 2.7. *The structure of the RLC data block – downlink*

– FBI (Final Block Identifier): this field is used to indicate that the block is the last to contain the RLC data.

– TFI: this field is used to identify the user of the data block.

– PR (Power Reduction): this field is used to indicate the reduction in power emitted for the next block.

– E (Extension): this bit indicates the presence of an optional field in the RLC header.

– BSN (Block Sequence Number): this field is used to number the RLC block modulo 128. The acknowledged mode is based on the principal of the transmission of blocks with an anticipation window (Figure 2.17).

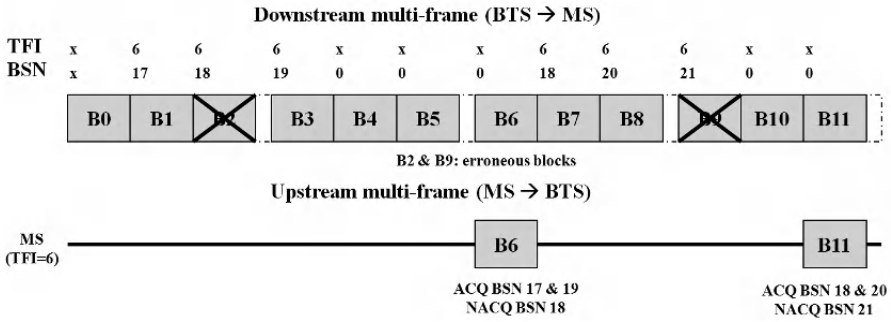


Figure 2.17. *The RLC acknowledgement procedure*

– M (More bit): this field indicates whether a new LLC data unit follows the current LLC data unit inside the same RLC/MAC data block.

– LI (Length Indicator): this field is used to demarcate the LLC frames when a RLC block contains more than one LLC frame.

The RLC sub-layer consists of the following fields the uplink (Table 2.8):

– TI (TLLI Indicator): this field indicates whether the TLLI optional field is present or not.

– PI (PFI Indicator): the bit indicates whether the PFI is present.

– TLLI: this field is used to identify the user of the block. This optional field is included in particular cases where the same TFI is assigned to two different mobiles.

– PFI (Packet Flow Identifier): this field contains a data flow identifier.

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
	PI	TFI					TI
BSN							E
LI						M	E
TLLI							
PFI							E
LLC data unit							

Table 2.8. *The structure of the RLC data block – uplink*

2.3.2.3. *Control data*

Control messages are directly encapsulated by the RLC/MAC header.

In the downlink, the RLC header contains the following additional fields (Table 2.9):

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Payload type		RRBP		S/P	USF		
RBSN	RTI					FS	AC
PR		TFI					D
Control message							

Table 2.9. *Encapsulation of the control message – downlink*

– AC (Address Control): this bit indicates the presence of the TFI/D optional field in the header of the downlink control data block.

– FS (Final Segment): this bit indicates that the control data block contains the last segment of the control message.

– RTI (Radio Transaction Identifier): this field indicates the segment number when a control message uses several RLC/MAC data blocks.

– D (Direction): this bit indicates whether the TFI is assigned to the uplink or the downlink.

– RBSN (Reduced Block Sequence Number): this bit indicates the sequence number of control data blocks for the downlink.

Table 2.10 describes the structure of the RLC header for the uplink.

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Payload type							R
Control message contents							

Table 2.10. *Encapsulation of the control message – uplink*

2.3.3. *The MS−SGSN interface*

2.3.3.1. *The LLC layer*

The LLC protocol is located at the level of the data link layer. The role of the LLC protocol is to convey information between the data entities located in the mobile and the SGSN. A LLC layer connection is identified by a SAPI service access point and is used to identify the TLLI of the mobile.

The LLC protocol provides six service access points for protocols of a higher level:

– four SAPIs are dedicated to the SNDCP that manages traffic data, corresponding to four levels of service quality;

– one SAPI is dedicated to signaling for the management of the mobility management and the SM session;

– one SAPI is dedicated to SMS text messages.

The LLC protocol provides the following functions:

– the transfer of data with acknowledgment;

– the transfer of data without acknowledgment;

– flow control;

– data encryption;

– erroneous frame detection.

2.3.3.1.1. The structure of the LLC frame

There are four types of LLC frame:

– the I frame for data transfer;

– the supervision S frame;

– the UI frame for the transfer of data without acknowledgment;

– the unnumbered U frame.

The header (see Table 2.11) is composed of:

– an address field containing the SAPI, coded on a byte;

– a field of variable length coded on a maximum of 36 bytes;

– a FCS (Frame Check Sequence) field coded on 3 bytes allowing it to monitor the frame errors.

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
SAPI (1 byte)							
Control (variable length, max. 36 bytes)							
Information (variable length, max. value negotiated)							
Frame check sequence (3 bytes)							

Table 2.11. *The structure of the LLC frame*

The S frame is used to acknowledge received data when there are no data to transmit. It is also used for flow control.

The I frame transports the data in acknowledgment mode. The numbered I+S frame also transports supervisory information. There are four types of supervisory mixed frame and I+S data frame:

– the RR (Receive Ready) frame indicates that the receiver is ready to receive I frames and acknowledges the I frames it has received previously;

– the ACK (ACKnowledgement) frame is used to acknowledge one or more I frames. It also indicates the loss of a frame in the received sequence;

– the SACK (Selective ACKnowledgement) frame contains a table indicating the frames that have been correctly received and those lost in the received sequence;

– the RNR (Receive Not Ready) frame indicates to the source that the receiver is not available to receive new data frames.

The U frame is used to achieve LLC protocol control functions. There are six different frames:

– the SABM (Set Asynchronous Balanced Mode) frame is used to establish the LLC connection in acknowledgment mode;

– the DISC (DISConnect) frame is used to terminate an LLC connection;

– the UA (Unnumbered Acknowledgement) frame is used to acknowledge a SABM or a DISC frame;

– the DM (Disconnect Mode) frame is used to indicate to the source that the receiver is unable to process the received command;

– the FRMR (FRaMe Reject) frame is used to inform the remote extremity that the rejected frame cannot be recovered by retransmission;

– the XID (eXchange IDentification) frame is used for parameter negotiation of the LLC protocol and the SNDCP protocol.

2.3.3.1.2. Data transfer

The acknowledgment mode is supported by all types of SAPI. It is always available once the LLC layer has received the TLLI identifier from the mobile. The LLC thus functions in ADM (Asynchronous Disconnected Mode). The GMM protocol and the SMS service only use the ADM.

Before using the acknowledged mode, a negotiation procedure must be undertaken. The LLC layer thus functions in ABM (Asynchronous Balanced Mode) and can also support the unacknowledged mode. The SNDCP protocol uses both the ABM and the ADM.

The data without acknowledgment can be transferred in ABM or ADM. They use the same UI frames. The LLC protocol must, however, separate the duplicated frames identified by a number present in the header of the LLC frame. The header of the LLC frame also indicates whether or not the frame is encrypted. Similarly, the header indicates whether an error control is used for the information field and the header or solely for the header. The LLC frame in unacknowledged mode is transmitted in RLC frames with or without acknowledgement.

The data with acknowledgement are transferred solely in ABM, which requires the establishment of a connection. During the establishment phase, several parameters are negotiated (window lengths, time switches and frame lengths).

The data with acknowledgment uses the I frames, which are encrypted if the GMM protocol has communicated the encryption information. Error control is

systematically carried out on the header and information field. The LLC frame with acknowledgment is transmitted in RLC frames with acknowledgment.

2.3.3.1.3. Encryption

The LLC protocol allows for transfer privacy by encrypting the information field and the FCS field (Figure 2.18) in:

– I frames when the TLLI identifier has been communicated to the mobile;

– UI frames if the encryption information has been communicated to the mobile and the GMM protocol indicates it.

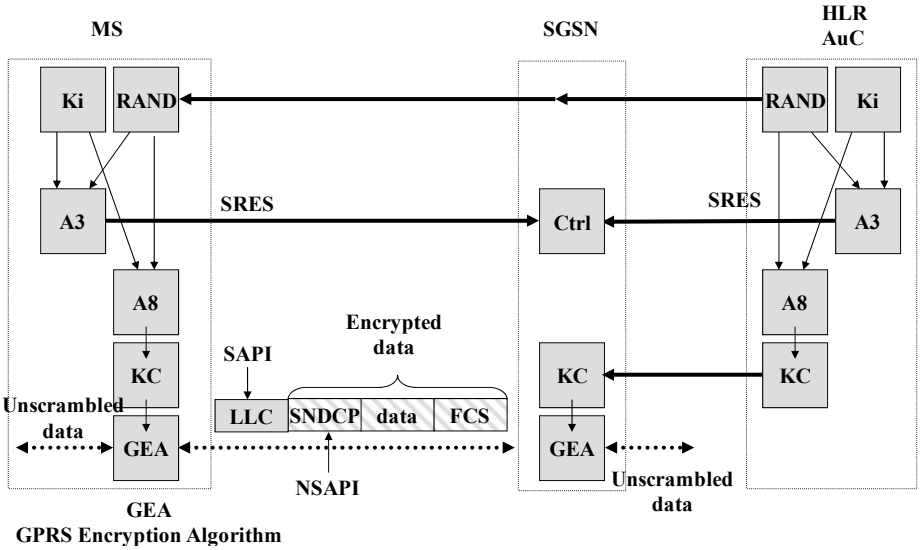


Figure 2.18. *Data encryption*

2.3.3.2. *The SNDCP layer*

The SNDCP layer allows the multiplexing of several service data units from different external networks (IP packets) on the same LLC link and enables their potential compression. The user's flow is identified by the NSAPI in the SNDCP header. The NSAPI connected to the TLLI is used to identify the PDP context that contains all of the information allowing for the transfer of data between the mobile and the GGSN.

The SNDCP carries out two types of compression:

– the compression of TCP/IP headers. In this instance it only transmits the difference between two consecutive headers;

– the compression of data.

2.3.3.2.1. Multiplexing

When a GPRS user wants to start the data transfer, a PDP context is activated for this purpose. The activation is made by the SM protocol. A NSAPI is reserved for the PDP and the data flow belonging to this connection is identified by the NSAPI. The SDNCP supports several simultaneous PDP contexts that can be connected to any four SAPIs of the LLC layer.

The NSAPI field is used for identification of the PDP type and for the PDP address pair. The MS (mobile station) dynamically allocates NSAPIs to the activation of the PDP context. The SNDCP entity transmitted inserts the NSAPI value for each data unit. The SNDCP entity uses the receiving NSAPI to identify the SNDCP user from the data unit.

The following SNDCP function combinations are permitted:

– one or more NSAPI can use a SAPI;

– only a SAPI will be used by a NSAPI.

2.3.3.2.2. LLC layer functioning management

The SNDCP layer is responsible for the establishment, reestablishment and release of the LLC layer with acknowledgment function. The reestablishment and release of the LLC layer with acknowledgment function can also be initialized by the LLC layer.

The XID parameter negotiation can be carried out simultaneously with the procedure of reestablishment or establishment. It is also possible to negotiate the XID parameters independently from the procedure of reestablishment or establishment.

2.3.3.2.3. The buffer memory of data units

For the transfer of data with acknowledgement, the SNDCP entity places a data unit in a buffer memory until it has been confirmed that all segments of the unit have been received. The stored correctly received and acknowledged data unit will be destroyed.

For data transfer without acknowledgment, the SNDCP entity deletes a data unit as soon as it has been delivered to the LLC layer.

2.3.3.2.4. Compression of the header

Compression of the protocol header of the service data unit is an optional function of the SNDCP. The negotiation of the supported algorithms and their parameters is carried out between the MS and the SGSN by using the XID parameters.

The header compression method is specific for each network layer protocol. The TCP/IP (IPv4) header compression is specified in the RFC 1144. The compression of TCP/IP (IPv4) and UDP/IP headers is specified in the RFC 2507.

The following SNDCP combinations are permitted:

– one or more NSAPIs can use the same header compression protocol;

– a NSAPI can use one, more or, no header compression protocol;

– a header compression entity will be connected to a SAPI.

2.3.3.2.5. Data compression

Data compression is an optional function of SNDCP. Data compression is carried out on an entire data unit, including the compressed header data. Data compression is specified by the V.42bis recommendation of the ITU-T (International Telecommunication Union – Telecom).

The following combinations of SNDCP functions are permitted:

– one or more NSAPI can use the same data compression entity;

– a NSAPI can use one, more or no data compression entity;

– separated data compression entities are used for data units;

– a data compression entity is connected to a SAPI;

– one or more header compression protocols can be connected to the same data compression entity;

– a header compression entity is connected to one, several or no data compression entity (entities).

2.3.3.2.6. Segmentation and reassembly

Segmentation is carried out by the SNDCP entity to ensure that no data unit transmitted is longer than the parameter negotiated by the LLC layer. The received SNDCP entity reassembles the segments of the data unit. The segmentation and

reassembly procedures are different for the mode depending on whether it is functioning with or without acknowledgment.

2.3.3.2.7. The structure of the SNDCP header

The SNDCP can use the LLC protocol in either acknowledged or unacknowledged mode. In the acknowledged mode, the header consists of 2 or 3 bytes. In the unacknowledged mode, the header consists of 3 or 4 bytes.

In the acknowledged mode, the SNDCP header contains the following fields (Table 2.12):

– the NSAPI access point;

– a M (More bit) indicator specifying whether or not the SNDCP data unit is followed by other units that are part of the same service unit (for segmentation);

– a T (Type bit) indicator specifying the header type, with or without acknowledgment;

– a F (First segment bit) indicator specifying whether or not it is about the first segment. The DCOMP (Data COMPression) and PCOMP (Protocol COMPression) fields only appear in the first segment;

– a X (spare bit) indicator. This bit is placed at ZERO;

– the references for the algorithms of DCOMP or of headers used (PCOMP). The negotiation between the mobile and the SGSN is carried out with the help of an LLC XID exchange frame.

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
X	F	T	M	NSAPI			
DCOMP				PCOMP			
Number of the service data unit							
Service data unit							

Table 2.12. *SNDCP data unit – acknowledge mode*

When the LLC protocol is used in unacknowledged mode, the header also includes a SNDCP data unit sequence number, which allows for a reliable reassembly of the segments (Table 2.13).

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
X	F	T	M	NSAPI			
DCOMP				PCOMP			
Sequence number				Number of service data unit			
Number of service data unit (continued)							
Service data unit							

Table 2.13. *The SNDCP data unit – unacknowledged mode*

2.4. Communication management

2.4.1. *Roaming management*

2.4.1.1. *Attachment to the network*

To access the GPRS network, the mobile must make the network aware of its presence with the help of a GPRS Attach procedure that aims to update the RAI and the mobile's P-TMSI. The RAI is a sub-assembly of the LAI (Location Area Identity). The SGSN will carry out an IMSI Attach procedure to update the parameters belonging to the GSM, the LAI location and the TMSI.

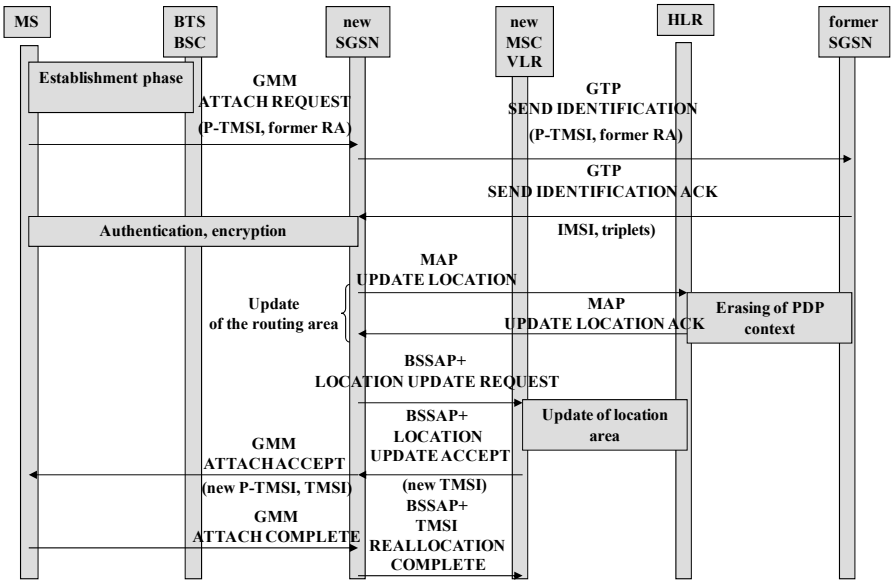


Figure 2.19. *Attachment of the mobile to the network*

The GPRS Attach procedure starts with the sending of an ATTACH REQUEST message at GMM level. The parameters provided by the mobile are the IMSI, if it does not have a P-TMSI, or the P-TMSI and the former identity of the routing area RAI if the mobile has changed SGSN. If the network does not possess a mobility context for the mobile, the new SGSN will request the identification of the mobile from the former SGSN and starts an authentication and encryption phase with the mobile (Figure 2.19).

The SGSN then begins a procedure to update the RAI in the HLR via the MAP protocol and the LAI in the MSC via the BSSAP+ (BSS Application Part) protocol. The LAI in the HLR is updated by the MSC.

The MSC indicates the new value of the TMSI to the SGSN in the LOCATION UPDATING ACCEPT message. The SGSN indicates the new value of the TMSI and P-TMSI to the mobile in the ATTACH ACCEPT message. The acknowledgment of the mobile with regard to the SGSN is carried out by the ATTACH COMPLETE message, and of the acknowledgment SGSN with regard to the MSC via the TMSI RASLLOCATION COMPLETE message (Figure 2.19).

When the GPRS Attach procedure is carried out, the mobile is in the READY state and the mobility contexts are established in the mobile and the SGSN. The mobile can thus activate the PDP contexts.

2.4.1.2. *Detachment from the network*

The detach procedure allows the terminal to inform the network that it wishes to detach from the GPRS network (GPRS Detach) and/or from the GSM network (IMSI Detach). It also allows the network to inform the mobile that it is detached from the GPRS or GSM network.

If a GPRS Detach procedure is involved, upon receiving the DETACH REQUEST message from the mobile at GMM level, the PDP contexts of the mobile are deactivated in the GGSN via the transmission of the GTP DELETE PDP CONTEXT REQUEST message. If an IMSI Detach procedure is involved, the SGSN sends a IMSI DETACH INDICATION message (Figure 2.20).

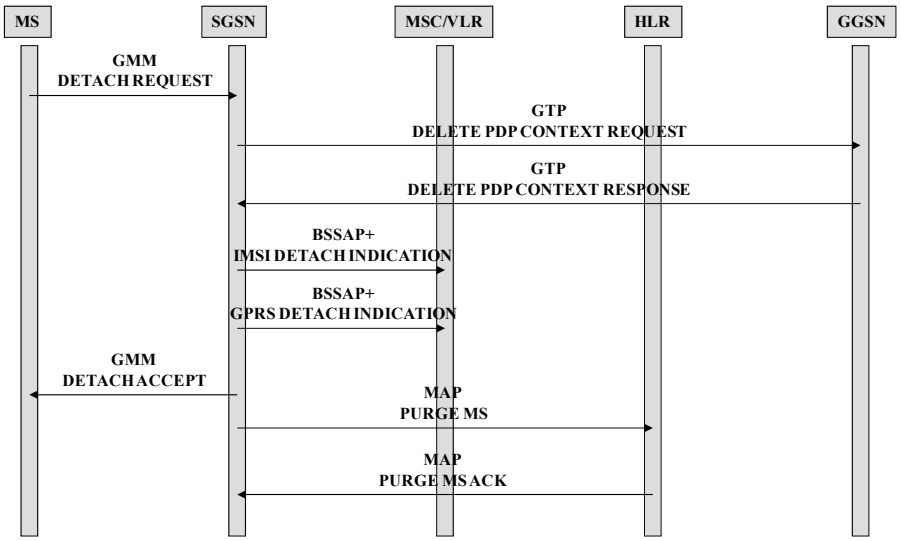


Figure 2.20. *Detachment of the mobile from the network*

If the terminal wishes to remain attached to the GSM network, the SGSN sends a detachment indication from the GPRS network to the MSC. The MSC removes the association with the SGSN and processes the paging and location without resorting to the SGSN.

The SGSN can sometimes keep the PDP and mobility contexts. These environments can be used with a new GPRS Attach without querying the HLR. The purge function allows the SGSN to inform the HLR that it has deleted the PDP context from the mobile via the MAP PURGE MS message (Figure 2.20).

2.4.2. *Session management*

2.4.2.1. *Activation of the PDP context by a mobile*

The activation of the PDP context creates the following stage in order to be able to exchange information with the external networks. This stage allows the mobile to be known by the GGSN gateway concerned. During the procedure, the mobile communicates the APN of the external network to which it wishes to connect. After verification, the SGSN establishes a PDP context, selects the GGSN and negotiates the quality of service. The call between the mobile and the external network can thus take place.

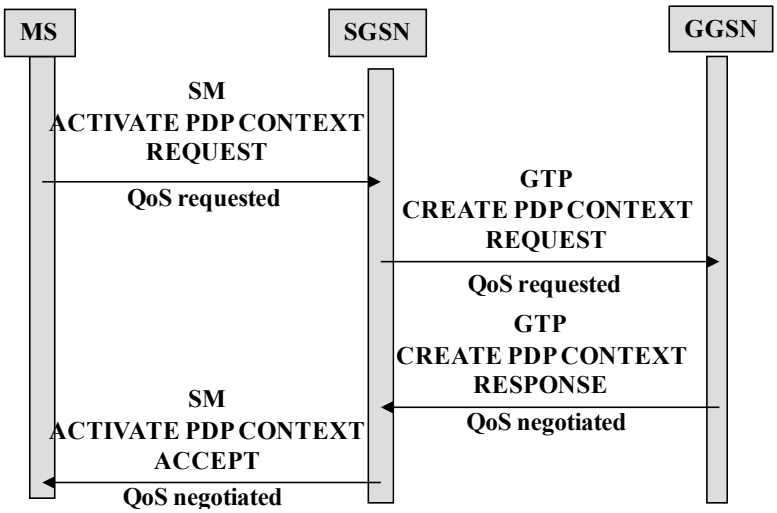


Figure 2.21. *Activation of the PDP context by the mobile (QoS – quality of service)*

The mobile transmits the SM ACTIVATE PDP CONTEXT REQUEST message that contains the features of the context. The SGSN finds the IMSI of the mobile and the GGSN concerned. It transmits the context and the IMSI to the GGSN in a GTP CREATE PDP CONTEXT REQUEST message (Figure 2.21).

From then on, the GGSN is capable of exchanging the mobile's data with the external network. The mobile may request a certain quality (loss, delay) to establish the context. The quality of service actually accepted by the network can be worse (Figure 2.21).

2.4.2.2. *Activation of the PDP context by the network*

The activation of the PDP context by the network corresponds to the instance when the external network wants to transfer data to the mobile whose PDP context is not activated. This can happen when the GGSN has stored the correspondence between the IP address and the IMSI of the mobile (Figure 2.22).

When the GGSN receives a data packet from an external network, it requests the IP address of the SGSN where the mobile is situated from the HLR via a MAP message. When this is recovered, the GGSN sends a GTP message to the SGSN to ask the mobile to activate the PDP context following the previous procedure. The SGSN sends a SM message to the mobile to initialize this procedure.

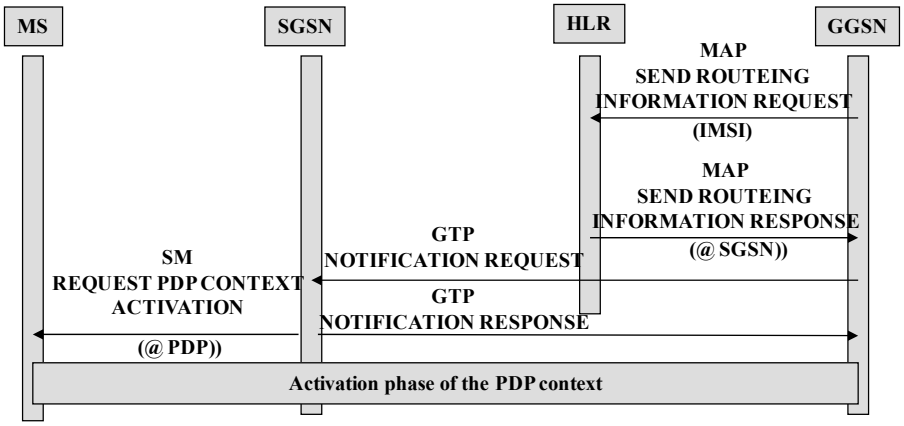


Figure 2.22. *Activation of the PDP context by the network*

2.4.3. *Traffic establishment*

2.4.3.1. *Establishment in the uplink*

In the case of one-phase access, the mobile transmits a PACKET CHANNEL REQUEST in random access on the PRACH or RACH logical channel. The request specifies the type (one-phase access, GMM signaling) and the multi-slot class of the mobile (Figure 2.23).

The network resends a PACKET UPLINK ASSIGNMENT message containing the PDCH logical channel, the flow identifier TFI and a USF (Uplink Status Flag) number, on the PAGCH or AGCH logical channel. The CS (CS1 to CS4) is specified in this message. The message also contains a TAI (Time Advance Indicator) index which enables the value of the phase advance in the PTCCH logical channel shared by all data flows to be found (Figure 2.23).

At this level, the mobile is no longer identified by the network during random access. To resolve the collision problems, the mobile places the random TLLI identifier in the RLC header that the network acknowledges as quickly as possible via the PACKET UPLINK ACK/NACK message on the PACCH logical channel.

The mobile can transmit the measurements carried out on the cell and neighboring cells by sending a PACKET MEASUREMENT REPORT message in the PACCH logical channel, inserted in the center of the data block. The frequency of the measurement reports is indicated by the network (Figure 2.23).

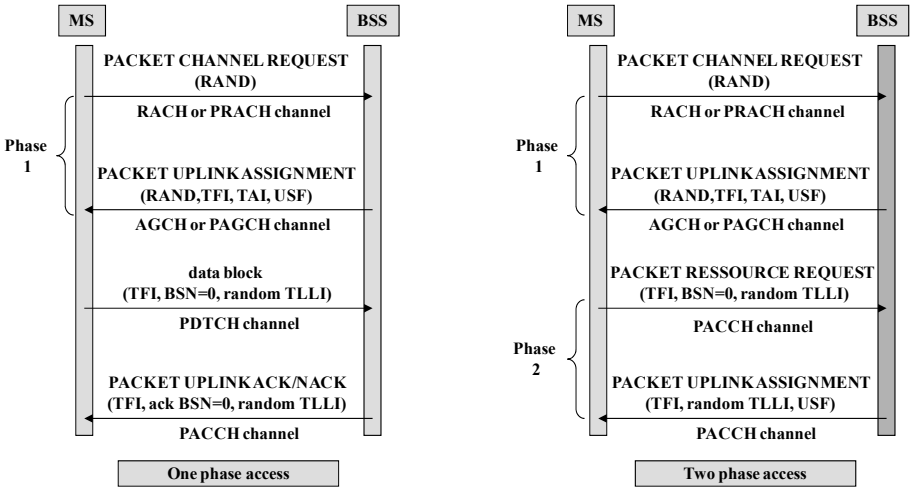


Figure 2.23. *Establishment procedures by the mobile*

The two phase access includes the initial random access phase and a subsequent phase where the mobile indicates the type of flow to transmit (requested rate, number of bytes to transmit, priority, acknowledge or unacknowledged mode at RLC level). The two phase access can be decided by the mobile in the PACKET CHANNEL REQUEST message or demanded by the network in the PACKET UPLINK ASSIGNMENT message (Figure 2.23).

When no resource is available, the network can queue the requests. It acknowledges the request of the mobile via the PACKET QUEUING NOTIFICATION message which is used to allocate a TQI (Temporary Queuing Identifier), the TFI only being allocated for effective data flow. When the resource becomes available, the network activates the data flow via a one or two phase mechanism (Figure 2.24).

As the mobile is likely to leave the cell, the network controls its presence via the PACKET POLLING REQUEST message transmitted on the PAGCH or AGCH logical channel and reserves the following block by means of a USF. The mobile responds via a PACKET CONTROL ACK message transmitted in the PACCH logical channel (Figure 2.24).

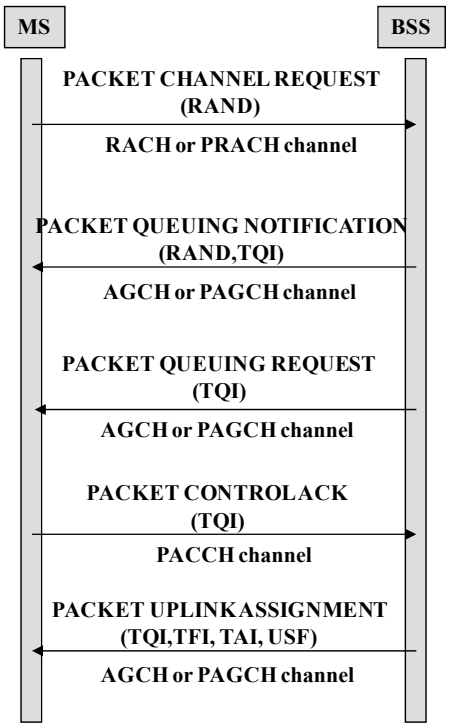


Figure 2.24. *The procedure of establishment with call-hold*

2.4.3.2. *Establishment in the downlink*

When the network wants to transmit a data flow to the mobile, two instances can arise:

– the mobility context is in the READY state, and the network knows the cell where the mobile is situated;

– the mobility context is in the STANDBY state, and the network only knows the routing area. The network must proceed to a broadcast call phase.

In the case of the establishment without paging phase, the network sends the PACKET DOWNLINK ASSIGNMENT message in the PAGCH or AGCH logical channel. The mobile is sent by its TLLI. The message contains the allocated TFI and the detailed description of the PDCH logical channel.

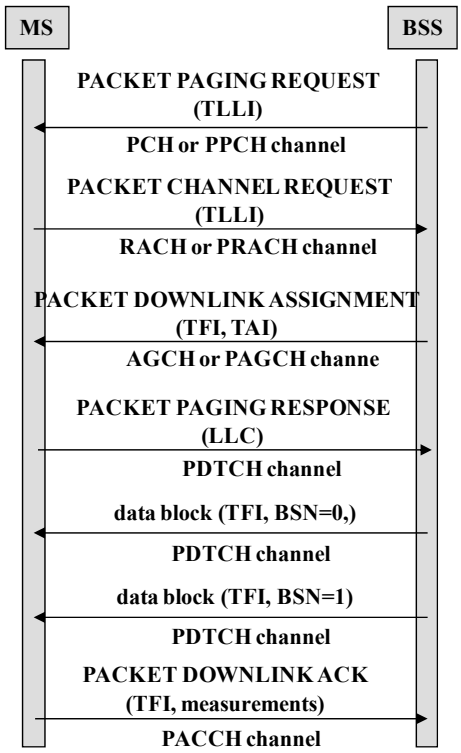


Figure 2.25. *The establishment procedures by the network*

If the network knows the TA, it also indicates this in the allocation message. In the opposite instance, it can use the polling mechanism. The mobile acknowledges the received data via the PACKET DOWNLINK ACK/NACK message which contains the measurements carried out on the cell and neighboring cells (Figure 2.25).

When the mobile is in STANDBY state, the network starts via a broadcast call phase with the PACKET PAGING REQUEST message containing the TLLI, on the PPCH or PCH logical channel. When this message is received, the mobile carries out a random access on the PRACH or RACH logical channel with a PACKET PAGING RESPONSE message which specifies that it is regarding a response to a paging (Figure 2.25).

2.4.4. *Location management*

The location of a mobile is achieved either at cell level, or at routing area level. The network must track the location of the mobile:

– when it changes cell inside the routing area (intra-area routing mobility);

– when it changes routing area without changing SGSN (inter-area mobility of intra-SGSN routing);

– when it changes routing area and attachment SGSN (inter-area routing mobility and inter-SGSN).

2.4.4.1. *Cell updating*

In the case of the GSM, the choice of cell on which the mobile can traffic is decided by the network. The change of cell is carried out by the network via the handover procedure.

In the case of the GPRS network, the selection of cell for a mobile without a data flow is made possible via the following three procedures:

– the mobile applies the selection process autonomously;

– the mobile applies the selection process and sends the radio field measurements;

– the mobile sends the radio field measurements and the network selects the cell.

2.4.4.2. *Intra SGSN updating*

When the mobile attached to a SGSN enters into a new routing area, an update of this is carried out. The SGSN does not alert the HLR of the mobile's new location.

The mobile sends an area update request to the SGSN via the GMM ROUTING AREA UPDATE REQUEST containing the former routing area and the former P-TMSI identifier. The BSS adds the identifier of the cell in which the message was received before passing the message onto the SGSN. The SGSN is capable of deducting the routing area from the cell's identifier.

The authentication and encryption functions are then carried out and a new P-TMSI identifier is allocated to the mobile. The SGSN updates a new mobility context.

2.4.4.3. *Inter SGSN updating*

When the mobile changes the routing area and SGSN, the previous procedure starts up on the new SGSN, which sends a GTP SGSN CONTEXT REQUEST

message to the former SGSN, to recover the PDP and mobility contexts. The authentication and encryption procedure between the mobile and the new SGSN is then initialized (Figure 2.26).

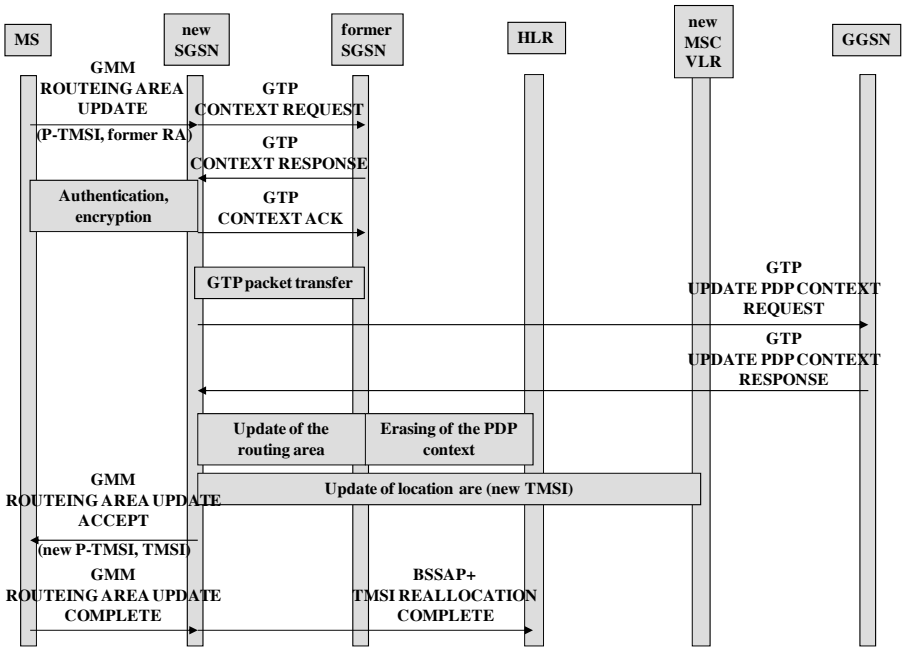


Figure 2.26. *Routing area updating*

The former SGSN starts up a tunnel in order to send the data which is sent by the former SGSN to the mobile to the new SGSN, for which an acknowledgment at LLC level was not received. They are redirected back to the mobile by the new SGSN. The data received by the former SGSN coming from the GGSN undergoes the same diversion.

The new SGSN requests an update of the PDP context from the GGSN via the GTP UPDATE PDP CONTEXT message, and informs the HLR of the SGSN change via the MAP UPDATE LOCATION message. The HLR requests the former SGSN to delete the data relating to the mobile (PDP context) (Figure 2.26).

The HLR once again sends the data relating to the mobile to the new SGSN via the MAP INSERT SUBSCRIBER DATA message, containing data belonging to the GSM (IMSI, MSISDN). The SGSN constructs the mobility and PDP contexts for this mobile and sends an acknowledgment back to the HLR (Figure 2.26).

When an association exists between the former SGSN and the MSC and the GSM circuit is not activated, the new SGSN must send a location update request to the MSC via the BSSAP+ LOCATION UPDATING REQUEST message (Figure 2.26).

2.5. The EDGE evolution

2.5.1. *The impact on the GSM/GPRS network*

EDGE is introduced in the GSM and GPRS networks in order to offer:

– a service in ECSD (Enhanced Circuit-Switched Data)[1] circuit mode; or

– a service in EGPRS (Enhanced GPRS) packet mode.

The objective of the EDGE function is to increase the rate on the radio interface by conserving the same radio channel width (200 kHz). The maximum rate offered is equal to 384 kbps (theoretically 473.6 kbps) when the eight time slots are concatenated.

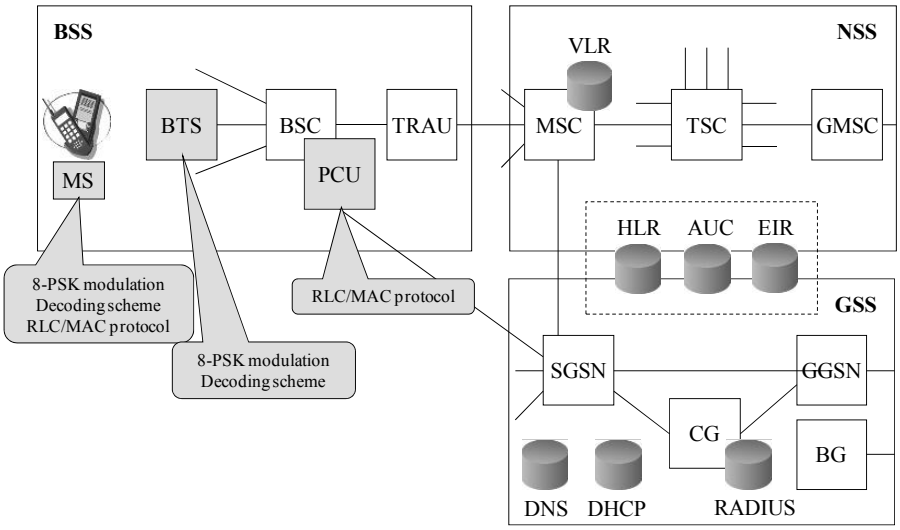


Figure 2.27. *The impact of EDGE on the GPRS network*

1 The following chapter does not cover the ECSD circuit mode.

This rate increase is made possible thanks to a new type of 8-PSK (Phase Shift Keying of 8 phase states) modulation and a new link adaptation mechanism for interference (Figure 2.27).

The GPRS and EGPRS networks use different RLC/MAC protocols between the mobile and the BSS sub-system. Specific messages are added to the protocol of RRC resource management. The impact of the introduction of the EDGE is located at BTS and BSC level (Figure 2.28).

The SGSN and the mobile use the same LLC, SNDCP, GMM and SM protocols for the GPRS and EGPRS types of network (Figure 2.28).

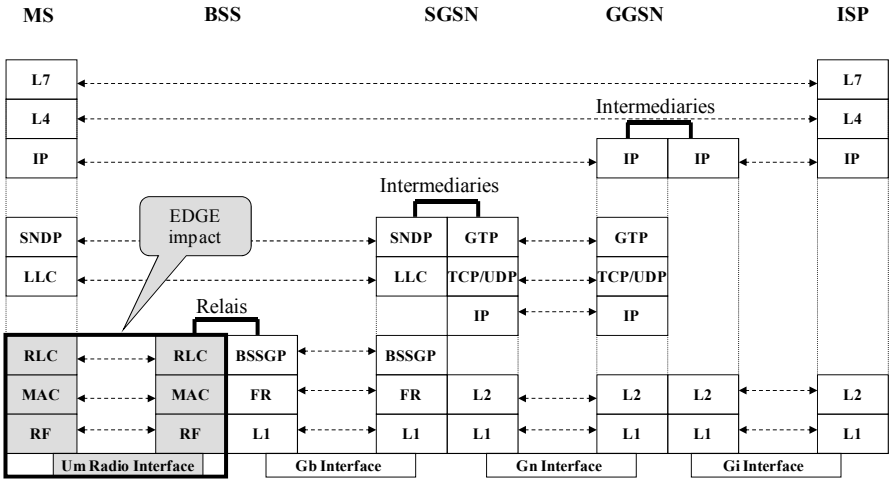


Figure 2.28. *The impact of EDGE on protocol architecture*

2.5.2. *Modification of the physical layer*

2.5.2.1. *Modulation*

The modulation used is of 8-PSK type. The transmitted radio carrier has eight phase states, each phase state (a symbol) representing a triplet of the binary signal to be transmitted. The symbol rate in 8-PSK has the same value as the rate in GMSK, or about 270.833 K symbols per second. The rate of the 8-PSK signal is therefore equal to 812.5 kbps (Figure 2.29).

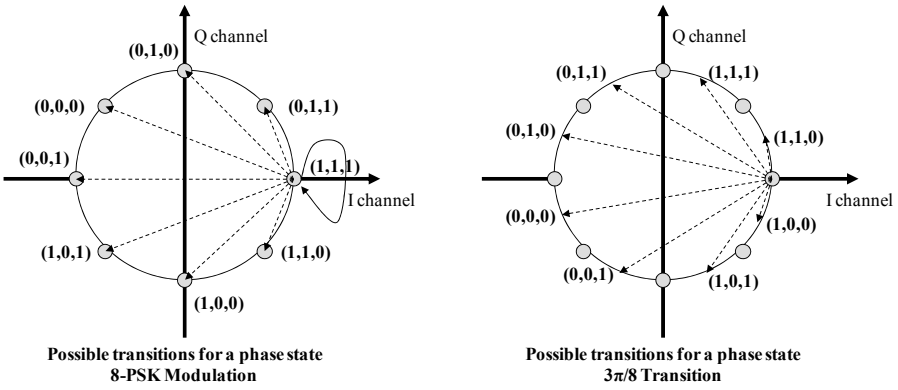


Figure 2.29. *The 8-PSK modulation*

In order to limit differences in amplitude when moving from one phase to another, a systematic rotation phase of $3\pi/8$ was introduced. Phase hopping is therefore in the form $3\pi/8 + k\pi/4$, the value of k depending on the value of the triplet.

To obtain a bandwidth compatible with the GMSK signal, the symbols are filtered before modulation.

2.5.2.2. *Channel coding*

The structure of the GSM burst is conserved whatever modulation is used. The burst is formed from a training sequence of 26 symbols, surrounded by 58 symbols of data on both sides. There are also three header and tail-end symbols, for ramp-ups and returns in reception, and 8.25 guard symbols. In the case of GMSK modulation, the symbol corresponds to a bit. In the case of the 8-PSK modulation, the symbol corresponds to 3 bits.

The data block derived from the RLC/MAC frame is transmitted in four bursts, which involves a data block length equal to:

– 58 bits * 2 *4 = 464 bits in the case of GMSK;

– 3 * 58 bits * 2 * 4 = 1 392 bits in the case of 8-PSK modulation.

Nine MCS (Modulation and Coding Scheme) channels are defined, which are numbered from 1 to 9. The GMSK modulation is used for MCS-1 to MCS-4. The 8-PSK modulation is used for MCS-5 to MCS-9 (Figure 2.30).

For each type of MCS, the following operations are carried out in order to form the data block:

– a convolutional code at a rate of 1/3 is applied to the RLC/MAC frame;

– puncturing is carried out on data from the encoder;

– the USF field is added;

– the pre-emption field is added.

The MCSs are grouped into different families − A, B and C − with different values relating to the size of the data unit: 37 bytes (A) (and 34 + 3 of stuffing), 28 bytes (B) and 22 bytes (C). For each MCS, a different number of data units is used to form the data of the RLC/MAC frame (one, two or four units), which allows for different bit rates. In the case of MCS-7, MCS-8 and MCS-9, the data block contains two RLC/MAC frames (Figure 2.30).

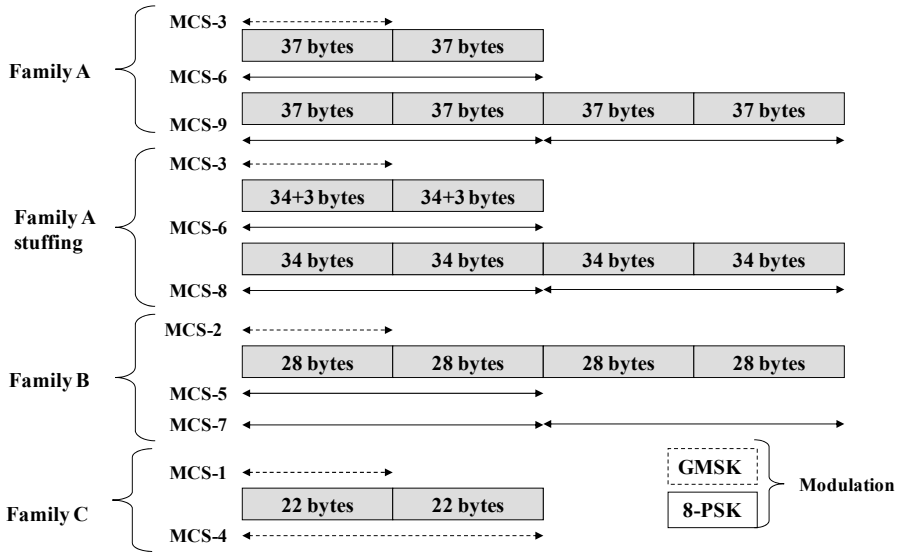


Figure 2.30. *The coding scheme families*

Each CS uses the same convolutional code (rate 1/3) but uses different puncturing. For each data bit, the encoder produces 3 output bits. The puncturing only conserves certain bits. To conserve the information, it is necessary to conserve a minimum of 1 in 3 bits (Table 2.14).

In order to ensure the best protection of the RLC/MAC header for interference, this is coded independently from the transmitted data (Table 2.14).

Coding scheme	Nominal rate (1 slot) in kbps	Data coding rate	Header coding rate
MCS-1	8.8	0.53	0.53
MCS-2	11.2	0.66	0.53
MCS-3	14.8	0.85	0.53
MCS-4	17.6	1.00	0.53
MCS-5	22.4	0.37	0.33
MCS-6	29.6	0.49	0.33
MCS-7	44.8	0.76	0.36
MCS-8	54.4	0.92	0.36
MCS-9	59.2	1.00	0.36

Table 2.14. *Coding parameters*

2.5.3. *Modification of the RLC/MAC layer*

For MCS-1, MCS-2, MCS-3, MCS-4, MCS-5 and MCS-6, there is a single RLC data unit.

There are three types of MAC/RLC headers defined according to the coding scheme:

– the type 1 header is used with MCS-7, MCS-8 and MCS-9. Several new fields are used for the GPRS header (see Tables 2.15 and 2.16):

- the ES/P (EGPRS Supplementary/Polling) field, which indicates whether the RRPB (Relative Reserve Block Period) field is valid or not, and what field the next control block in the uplink must contain,

- the CPS (Coding and Puncturing Scheme) field, which indicates the puncturing type for each MCS type and for each block of RLC data,

- the RSB (Resent Block Bit) field indicates whether a RLC data block is subject to a retransmission,

- two fields − BSN1 (Block Sequence Number) and BSN2 − transport the sequence number of two RLC data blocks;

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
TFI	RRBP		ES/P		USF		
BSN1		PR		TFI			
BSN1							
BSN2							BSN1
CPS					BSN2		

Table 2.15. *The structure of the type 1 header – downlink*

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
TFI		CV				SI	R
BSN1					TFI		
BSN2		BSN1					
BSN2							
	PI	RSB	CPS				

Table 2.16. *The structure of the type 1 header – uplink*

– the type 2 header is used with MCS-5 and MCS-6 (see Tables 2.17 and 2.18);

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
TFI	RRBP		ES/P		USF		
BSN1		PR		TFI			
BSN1							
				CPS			BSN1

Table 2.17. *The structure of the type 2 header – downlink*

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
TFI		CV				SI	R
BSN1					TFI		
CPS		BSN1					
					PI	RSB	CPS

Table 2.18. *The structure of the type 2 header – uplink*

– the type 3 header is used with MCS-1, MCS-2 MCS-3 and MCS-4 (see Tables 2.19 and 2.20). A new SPB (SPlit Block) field is used regarding the GPRS header. This field indicates whether the data are transmitted using resegmentation;

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
TFI	RRBP		ES/P		USF		
BSN1		PR		TFI			
BSN1							
	SPB		CPS				BSN1

Table 2.19. *The structure of the type 3 header – downlink*

Bit							
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**
TFI		CV				SI	R
BSN1					TFI		
CPS		BSN1					
		PI	RSB	SPB		CPS	

Table 2.20. *The structure of the type 3 header – uplink*

Unlike the GPRS, where the format of the RLC/MAC header is fixed, the EGPRS header has a variable size in addition to a HCS (Header Check Sequence) control sequence. Data from the LLC layer are segmented into blocks by the RLC layer and controlled by a BCS control sequence.

The convolutional code is applied to the RLC/MAC header complete with its control sequence and to RLC data completed with the following fields:

– FBI (Final Block Indicator) and E (End) identical to the RLC header fields in the GPRS;

– HCS, data check sequence;

– T, Trail bits of the convolutional code.

Several types of puncturing can occur within the RLC data according to the CS. A single type of puncturing is transmitted and it undergoes an interleaving either on four bursts (MCS-1 to MCS-6) or on 2 bursts (MCS-7 to MCS-9). This last instance corresponds to the sending of two RLC data units in a block (Figures 2.31 and 2.32). The encoded RLC/MAC header is completed by the USF field and the indication of the SB (Stealing Bits) CS and is interlaced on four bursts.

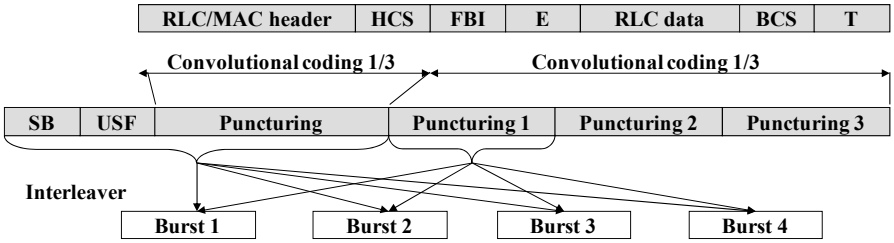


Figure 2.31. *The coding modes – interleaving on four bursts*

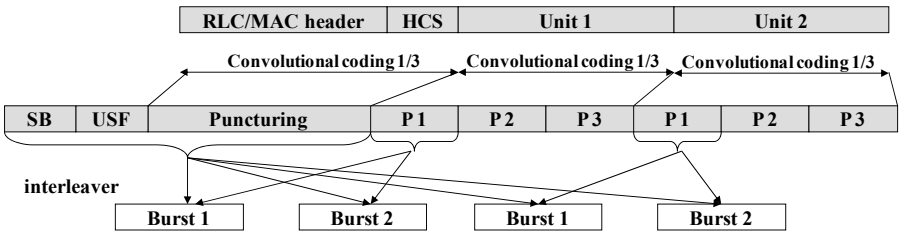


Figure 2.32. *Coding modes – interleaving on two bursts*

2.5.4. *Link control*

2.5.4.1. *Adaptation of the link*

To use a link at peak capacity, the mobile adapts the CS to the quality of the signal received by the BTS and applies it to a block. Resegmentation of the block is

not possible in the GPRS. When a block has erroneously been received, it must be retransmitted with the same CS.

One improvement brought by the EGPRS is the possibility to retransmit an improperly decoded block with a more robust CS. The transitions between CSs of the same family are possible.

The segmentation of an LLC data unit by the RLC protocol gives rise to numbering of the blocks. In the case of withdrawal on a more robust CS, the block to be repeated is cut into two sub-blocks. The two sub-blocks carry the same number, but a field in the RLC header is used to specify which part is involved.

2.5.4.2. *Incremental redundancy*

When a received block is erroneous, the receiver requests its retransmission with the same CS, but using a different type of puncturing. The receiver can thus apply the error-correcting mechanism on two or three types of different puncturing from the same RLC data unit (Table 2.21).

Coding scheme	**Coding rate P1**	**Coding rate P1 + P2**	**Coding rate P1 + P2 + P3**
MCS-1	0.53	0.26	-
MCS-2	0.66	0.33	-
MCS-3	0.85	0.42	0.28
MCS-4	1.00	0.50	0.33
MCS-5	0.37	0.19	-
MCS-6	0.49	0.24	-
MCS-7	0.76	0.38	0.25
MCS-8	0.92	0.46	0.21
MCS-9	1.00	0.50	0.33

Table 2.21. *Incremental redundancy*

Chapter 3

The UMTS Network

In this chapter, section 3.1 explains the services provided by the UMTS (Universal Mobile Telecommunications System) network, the main ones being the telephone service and the data transmission service. These services are implemented in CS (Circuit Service) or PS (Packet Service) mode, solely for data transmission.

Section 3.2 explains the architecture of the UMTS network, which consists of two sub-systems. As for the GSM (Global System for Mobile) and GPRS (General Packet Radio Service) networks, the core network includes the Network Sub-Systems (NSS) and GPRS Sub-Systems (GSS). The access network UTRAN (UMTS TRAnsport Network) provides a new technique for the allocation of a radio source to a flow.

Section 3.3 explains the radio interface between the mobile and the UMTS network. The description of the transmission chain essentially concerns the data link protocols, multiplexing by physical channel codes, modulation and frequency plan.

Section 3.4 describes the procedures limited to the UTRAN. Such procedures concern resource establishment for signaling or traffic, the implementation of the soft handover, the relocation of the anchor point and the inter-system handover.

Section 3.5 explains the HSPA (High Speed Packet Access) evolutions, which consist of an increase in rate via a new type of modulation, the concatenation of several physical channels and the exploitation of several propagation paths.

3.1. The services

The UMTS network offers a range of services divided into core network bearer services and RAB (Radio Access Bearer) services.

The bearer services allow for the transfer of three types of teleservice (Table 3.1):

– audio-frequency signal (300-3,400 Hz) for speech transfer. This service uses the CS circuit mode. The codec at a variable AMR (Adaptive MultiRate) replaces those used in the GSM network;

– UDI (Unrestricted Digital Information) signal. This service offers a rate of 64 kbps and uses the CS circuit mode. It is equivalent to the High-Speed Circuit Switched Data service of the GSM network;

– IP (Internet Protocol) packet. This service offers a rate ≤384 kbps and uses the PS packet mode. It is the equivalent of the EGPRS (Enhanced GPRS) service.

Teleservice	Class of service	Mode CS/PS	Maximum rate in kbps	
			Upstream	Downstream
AMR speech	Conversational	CS	12.2	12.2
UDI	Conversational	CS	64	64
Packet	Interactive	PS	64/128/384	64/128/384
	Background		8	8

Table 3.1. *The UMTS services*

The conversational class of service is used for real-time bi-directional signals, such as telephony or videoconferencing. Real-time applications have severe constraints on three quality-of-service parameters: loss, delay and jitter.

The streaming class of service is used for real-time unidirectional signals, such as real-time video or audio. This class of service presents less considerable constraints regarding delay.

The interactive class of service is used for applications where a user maintains a dialog with the server. Interactive applications generally use the TCP (Transport Control Protocol), which carries out recovery in the case of loss. The interactivity of these applications imposes a clause on the delay.

The background service class is used for Internet applications (email and file transfer), which are not very sensitive to deterioration in quality of service parameters.

3.2. The architecture of the network

3.2.1. *Network components*

The UMTS network has structure similar to that of the GSM and GPRS networks:

– the NSS is shared by GSM and UMTS networks for circuit-oriented services;

– the GSS is shared by the GPRS and UMTS networks for packet-oriented services;

– the access UTRAN has a topology that is practically identical to that of the Base Station Sub-system of the GSM and GPRS networks;

– the UE (User Equipment) mobile.

3.2.1.1. *The access network*

The access UTRAN and the user terminal support new protocols belonging to the UMTS. Numerous NSS and GSS features, however, come from GSM and GPRS networks.

The radio access UTRAN consists of the following elements (Figure 3.1):

– The RNC (Radio Network Controller): this ensures functions similar to those of the BSC (Base Station Controller) of the GSM and GPRS networks. It manages the radio resources for the area that it is controlling. It links up to the MSC (Mobile-services Switching Center) on the Iu_CS interface and to the SGSN (Service GPRS Support Node) on the Iu_PS interface. The Iur interface is used to directly connect two RNCs;

– Node B: this carries out functions similar to those of the Base Transceiver Station of the GSM and GPRS networks. It ensures the Uu radio interface with the mobile and links up to the RNC on the Iub interface.

A connection between a mobile and the core network (NSS or GSS) can use the resources of two RNCs, each one having a specific role. The SRNC (Serving RNC) manages the connection with the core network on the Iu_CS or Iu_PS interface, the signaling protocol with the mobile and the allocation of radio resources. The DRNC (Drift RNC) carries out the data transfer in a transparent manner between the Iub interface and the Iur interface and ensures the control of cells. The Iur interface is used to achieve the handover between two RNCs without resorting to the MSC or the SGSN.

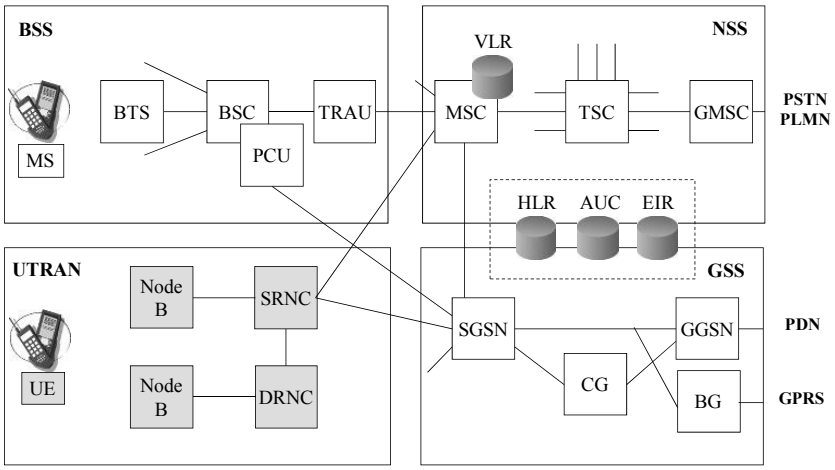


Figure 3.1. *The architecture of the UMTS network*

During a softer handover, the mobile is situated in a coverage area shared by two adjacent sectors of the same Node B. Communications between Node B and the mobile simultaneously borrow two radio channels. In the downlink, Node B must use two different codes so that the mobile can distinguish the signals from two sectors. The RAKE receiver of the mobile compensates for the delay and phase difference between the signals, before combining them. In the uplink, Node B receives signals from the mobile on two sectors, which the RAKE receiver of Node B combines (Figure 3.2).

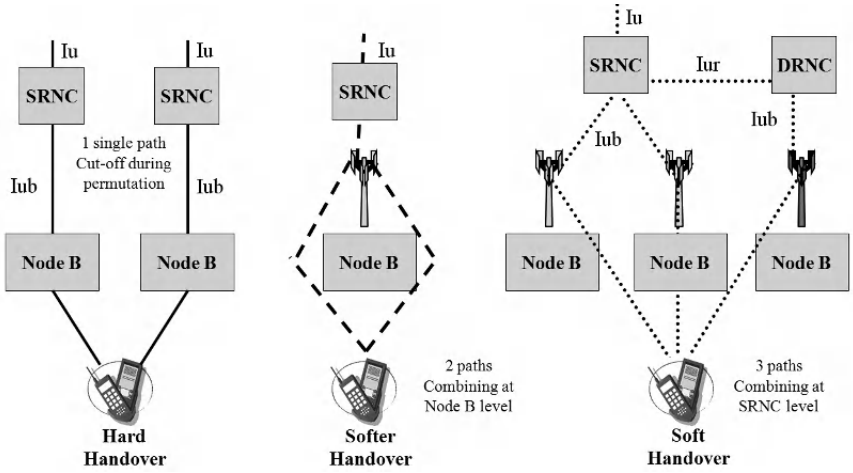


Figure 3.2. *The handover*

During a soft handover, the mobile is located in a coverage area shared by two B Nodes. In the downlink, there is no difference between the soft and the softer handover. Upstream, the mobile signal received by both B Nodes is transferred to the RNC, which selects the best frame. When both B Nodes are linked up to two RNCs, the SRNC that allocated the radio resource selects between signals coming from Node B and the DRNC that carries out a transit on the Iur interface (Figure 3.2).

3.2.1.2. *The mobile*

The UE mobile is composed of the following two parts:

– the ME (Mobile Equipment) mobile terminal corresponds to the radio terminal used for communication with the network;

– the UMTS Subscriber Identity Module is integrated in the smart UICC (Universal Integrated Circuit Card). It stores the subscriber's identity, the algorithms and the encryption keys, and certain data relating to the subscription of the user. The UICC also stores the Subscriber Identity Module, which contains the user data when they use the GSM and GPRS network.

Several types of bimode terminal (GSM/GPRS and UMTS) are defined:

– type 1: when the mobile is in a mode (GSM/GPRS or UMTS), the inactive part of the radio does not carry out any reception quality measurement. The transition from one mode to another requires the intervention of the user;

– type 2: when the mobile is in a mode (GSM/GPRS or UMTS), the inactive part of the radio can carry out reception quality measurements in order to automatically toggle;

– type 3: this type of terminal can simultaneously receive the information in two modes. Simultaneous transmission by both modes, however, is not possible.

– type 4: this type of terminal allows for simultaneous transmitting and receiving in both nodes.

3.2.2. *Protocol architecture*

The access stratum regroups the functions belonging to the UTRAN. It includes the radio network protocols that manage the bearer services for RAB[1] access:

– RRC (Radio Resource Control) between the mobile and the RNC;

1 The description only concerns the radio network protocols. The transport network protocols are mentioned in the figures purely for guidance.

– NBAP (Node B Application Part) between Node B and the RNC;

– RANAP (Radio Access Network Application Part) between the RNC and the MSC or SGSN;

– RNSAP (Radio Network Sub-system Application Part) between the SRNC and the DRNC.

The NAS (Non Access Stratum) is a set of protocols that enable the exchange of signaling information between the mobile and the core network[2]:

– CM (Call Management) and MM (Mobility Management) for the CS (Circuit Service) domain;

– SM (Session Management) and GMM (GPRS Mobility Management) for the PS domain.

3.2.2.1. *The Iu interface*

The Iu interface relies on the RNC and the MSC for circuit domain (Iu_CS) and SGSN for the packet domain (Iu_PS). The Iu_CS interface offers a communication control plane, a transport network control plane and a user plane (Figure 3.3). The Iu_PS interface offers a communication control plane and a user plane (Figure 3.4).

The RANAP protocol is the signaling protocol of the Iu interface communication control plane. It provides the following functions:

– the management of RABs including the initialization of the RAB, the modification of these characteristics and their suppression;

– paging broadcast to several B Nodes, sent by the network with the mobile identifier and its paging area;

– management of the hard handover between two MSCs or two SGSNs;

– reselection of the SRNC corresponding to the transfer of control functions from a mobile of one RNC to another RNC;

– transfer of signals exchanged between the mobile on the one hand and the MSC (CM, MM signaling) and the SGSN (GMM, SM) on the other;

– the activation and the deactivation of encryption and authentication functions.

2 The signaling protocols of the non access stratum correspond to those described in the GSM and GPRS networks.

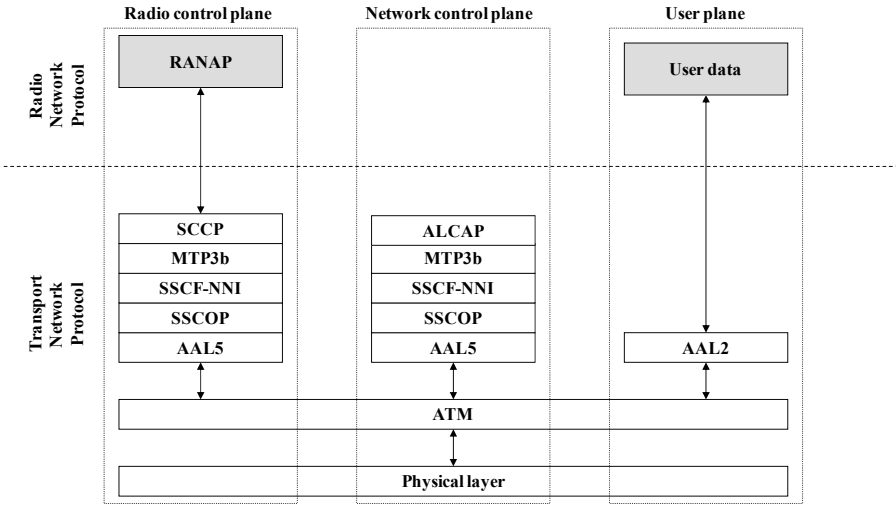


Figure 3.3. *The structure of the Iu_CS interface protocols*

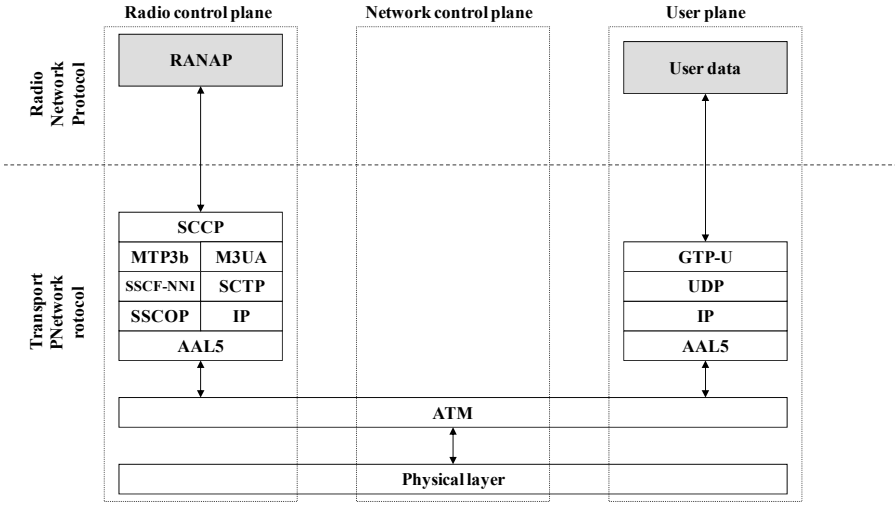


Figure 3.4. *The structure of the Iu_PS interface protocols*

3.2.2.2. *The Iub interface*

The Iub interface offers a communication control plane, a transport network control plane and a user plane (Figure 3.5). The NBAP protocol is the signaling

protocol of the communication control plane of the Iub interface. The NBAP protocol is divided into two components: the common component and the dedicated component.

The common component is used for signaling that does not concern the context of a mobile, such as alarm management of Node B or cell configuration or the transfer of specific measurements back to Node B.

The dedicated component is used when the RNC requests the establishment of a radio line for a mobile (code allocation), for alarm management and to transfer the specific measurements back to a radio link. It is also used in the implemention of the softer handover.

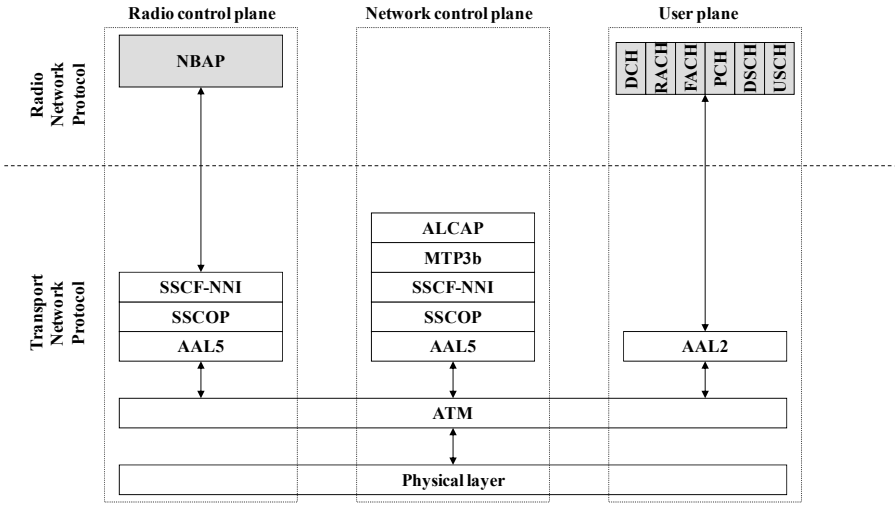


Figure 3.5. *The structure of Iub interface protocols*

3.2.2.3. *The Iur interface*

The Iur interface offers a communication control plane, a transport network control plane and a user plane (Figure 3.6). The RNSAP protocol is the signaling protocol of the Iur interface communication control plane.

The RNSAP protocol ensures the following functions:

– mobility management of a mobile between two RNCs, including the reselection function of the RNC, inter-RNC paging and management of protocol errors;

– the establishment, modification and release of dedicated traffic channels between both RNCs for the implementation of soft handover and the management of associated radio connections;

– the transfer of measurements concerning the cells.

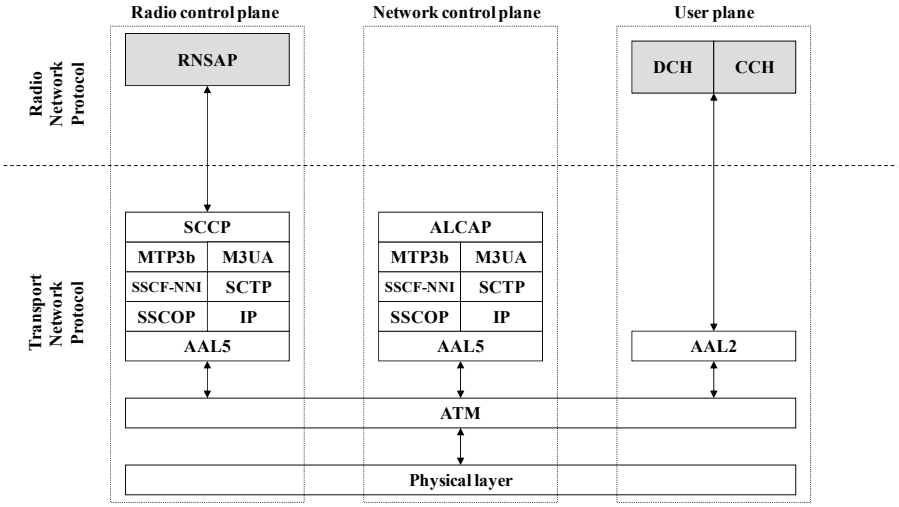


Figure 3.6. *The structure of the Iur interface protocols*

3.2.2.4. *The Uu interface*

The Uu interface offers a communication control plane and a user plane (Figure 3.7). The physical layer, the MAC (Medium Access Control) layer and the RLC (Radio Link Control) layer are shared by two user planes.

The physical layer offers services to the MAC layer via transport channels. The MAC in turn offers services to the RLC layer via logical channels. The RLC layer offers services to top layers via SAPI service access point identifiers.

On the control plane, the RLC services are used by the RRC layer. On the user plane, the RLC services are used by the PDCP (Packet Data Convergence Protocol) layers, BMC (Broadcast/Multicast Control) or by functions belonging to a user plane, such as the voice encoder.

The RRC layer supports the signaling exchanges between the mobile and the RNC for radio resource management, for paging and system information transmission and for the control of security functions. It carries out the transmission

of messages from the superior layers exchanged between the mobile and the MSC (CM, MM messages) or the SGSN (GMM, SM messages).

The PDCP layer is used at user plane level for packet domain services. It consists of different data compression methods (for example the TCP/IP headers), and supports the RNC reselection procedure without losing information.

The BMC layer is in charge of broadcast services on the radio interface such as the SMS text message service.

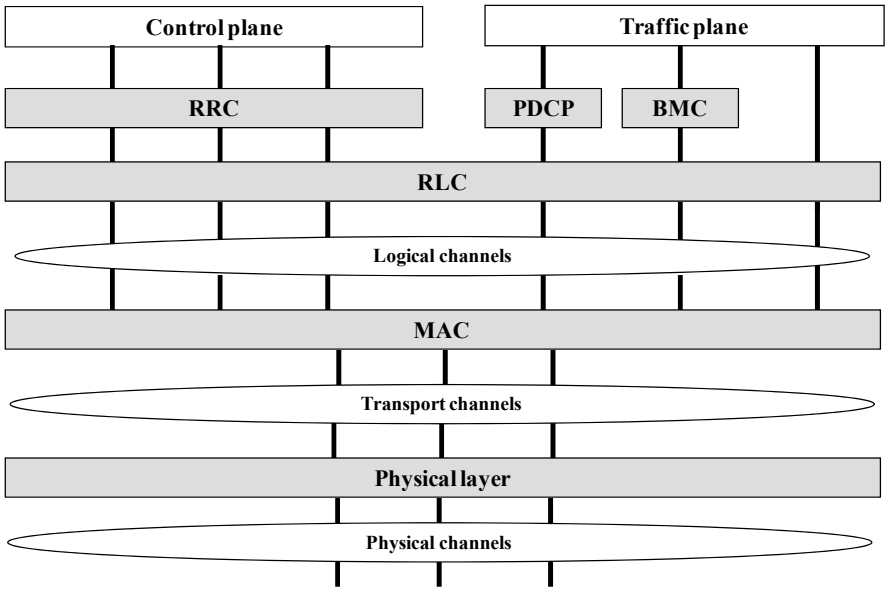


Figure 3.7. *The structure of Uu interface protocols*

3.2.3. *The femtocell*

The femtocell is a cell of small size obtained from a small HNB (Home Node B) radio station using the ISP (Internet Service Provider) access network to connect to a HNB-GW (HNB GateWay), Figure 3.8.

The HNB station is a standalone device or a function integrated into an integrated access device that provides triple play services (telephony, television and Internet access) from the ISP. It allows for the extension of UMTS network coverage indoors.

The UMTS mobile connects to the HNB station as a Node B via the Uu interface. The HNB-GW is seen by the NNS or GSS core network as a RNC, through the Iu_CS and Iu_PS interfaces.

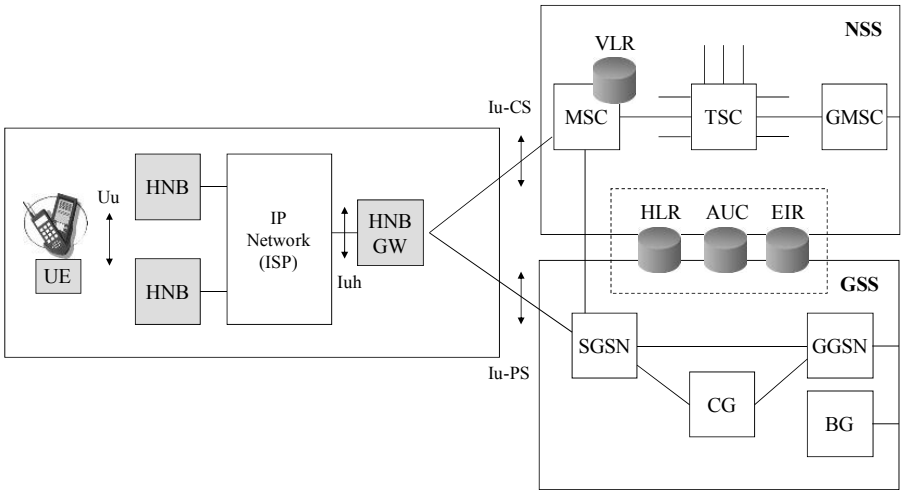


Figure 3.8. *The architecture of the Femtocell network*

The Iuh interface between the HNB station and the HNB-GW ensures the transport of control and traffic plane information for packet or circuit-oriented services (Figure 3.9).

The RANAP protocol, which is used for RAB establishment, is transported to the HNB station via the RUA (RANAP User Adaptation) protocol that ensures the establishment of a connection for NAS signaling transport of the mobile and RANAP messages.

The HNBAP protocol is exchanged between the HNB stations and the HNB-GW in order to transport information regarding the registration of radio stations.

The Uu radio interface PDCP/RLC/MAC layers are terminated at HNB station level. The traffic data in CS mode (the channel) is encapsulated on the Iuh interface by the RTP/UDP/IP headers. The traffic data in PS mode (IP packets) are encapsulated by the GTP/UDP/IP headers.

The RRC layer of the Uu radio interface is also terminated at HNB station level. The control data (RANAP, HNAP and NAS signaling) is encapsulated on the Iuh interface by the SCTP/IP headers.

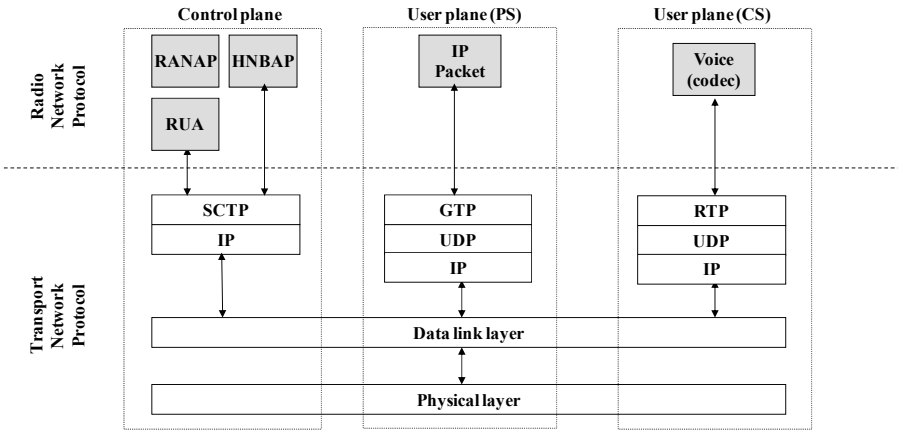


Figure 3.9. *The structure of the Iuh interface protocols*

3.3. Radio interface

3.3.1. *The RRC protocol*

3.3.1.1. *Connection states*

In the GSM, there are two connection states: the connected state and the standby state. In the GPRS there are three session states: the idle state (inactive state), the ready state (state corresponding to data transmission) and the standby state (state following the end of data transmission). In the UMTS, the following states are defined (Figure 3.10):

– a single idle state in disconnected mode;

– the CELL_DCH (Dedicated CHannel), CELL_FACH (Forward Access CHannel), CELL_PCH and URA_PCH states in connected mode.

The CELL_DCH state is a similar to the connected state of the GSM network. In this state, dedicated channels are allocated for both directions of communication and the mobility of the terminal is controlled by the network.

In the CELL_PCH and URA_PCH states, no dedicated resource is allocated to the mobile. In the CELL_PCH state, the position of the mobile is known at cell level. In the URA_PCH state, the position of the mobile in an area is known. Both CELL_PCH and URA_PCH location states provide additional flexibility in location management:

– a slow mobile uses the CELL_PCH state;

– a fast mobile uses the URA_PCH state.

In the CELL_FACH state, no dedicated resource is allocated to the mobile. The mobile can transmit data on the RACH (Random Access CHannel) or FACH transport channels.

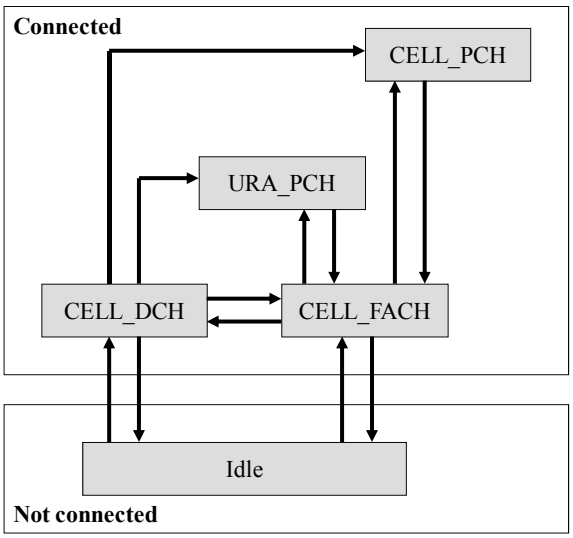


Figure 3.10. *The states of the RRC protocol*

3.3.1.2. *Functions*

The RRC protocol ensures the transmission of the following information on the BCCH in each of the network's cells:

– the core network information (identity of the Public Land Mobile Network);

– the selection/reselection parameters of cells and information about the neighboring cells;

– the features of common channels used in the cell;

– the control information regarding the measurements to be carried out by the mobile;

– the identity of the location areas URA (UTRAN Registration Area) to which the cell belongs.

The RRC protocol carries out paging management on the PCCH (Paging Control CHannel or the DCCH (Dedicated Control CHannel) of the incoming call intended for the mobile and the notification of the modification of system information.

The RRC protocol provides management for all mobilized resources (radio bearer, transport channel and physical channel). The configuration of resources is always initiated by the network.

The RRC protocol controls the different types of measurements that condition mobility management or reconfiguration of the radio bearer:

– measurements of reception power on the current and neighboring cells used by the mobile for cell reselection management and by the UTRAN for handover management;

– measurements of outgoing traffic on mobile transport channels concerning the level to which the transmission memory of the RLC layer is filled and the increase in resources allocated to the mobile (from a RACH to a DCH);

– quality measurements, such as the level of error when receiving transport blocks (BLER or BLock Error Rate).

The RRC protocol also conducts mobility control, see Table 3.2.

RRC states	Mobility control	Identification of the mobile	Location of the mobile
Idle	By the mobile according to selection−reselection rules broadcasted by the network	Unknown mobile	Unknown
CELL_FACH CELL_PCH	By the mobile according to selection−reselection rules broadcasted by the network	U-RNTI identifier assigned to the mobile	Cell update procedure executed by the mobile's RRC layer
URA_PCH	By the mobile according to selection−reselection rules broadcasted by the network	U-RNTI identifier assigned to the mobile	Cell update procedure executed by the mobile's RRC layer
CELL_DCH	By the RNC according to measurement results provided by the mobile (triggering a handover)	U-RNTI identifier assigned to the mobile	Active set update procedure executed by the RRC layer of the RNC

Table 3.2. *Mobility check*

3.3.2. *RLC protocol*

The RLC protocol ensures traffic and control data transmission functions between the mobile and the RNC. Three modes are possible:

– transparent mode: the RLC frame has no header and is composed of data from the top layer alone;

– unacknowledged mode: the RLC protocol achieves the segmentation or concatenation of data from the top layer, controls the sequence number (SN) and carries out encryption;

– acknowledged mode: the RLC protocol, in addition to the unacknowledged mode, carries out the acknowledgment of received frames, flow control and error correction via retransmission.

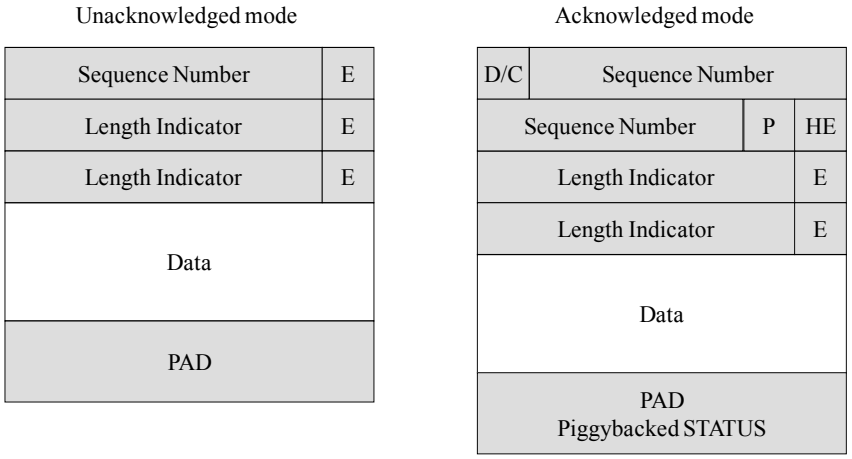


Figure 3.11. *The structure of the RLC header*

The RLC header, in acknowledged or unacknowledged mode, encapsulates RRC messages, PDCP or BMC frames, or speech signals. It consists of the following fields (Figure 3.11):

– Sequence Number: this field is used to reassemble the frames received;

– E (Extension): this field indicates whether the next field contains length indicator information;

– Length Indicator: this field is used to define the size of the data encapsulated;

– D/C: this field indicates whether the RLC frame is a data or control frame;

– P (Polling): this field is used to request a state report from the receiver;

– HE (Header Extension): whether the next field contains length indicator information.

Control frames are used in conjunction with the acknowledged RLC data frames. They allow for the acknowledgment of received data frames, the control of flows and the correction of errors via retransmission.

The different logical channels corresponding to RLC frames are described in Table 3.3.

Logical channel	Function	Mode
BCCH (Broadcast Control CHannel)	Common unidirectional channel used for the transmission of system information to mobiles	Transparent
PCCH (Paging Control CHannel)	Common unidirectional channel used to transmit paging messages to mobiles	Transparent
CCCH (Common Control CHannel)	Common bidirectional channel used to transmit control information to mobiles	Transparent or unacknowledged
DCCH (Dedicated Control CHannel)	Dedicated bidirectional control channel for the exchange of control information with mobiles	Transparent, acknowledged or unacknowledged
DTCH (Dedicated Traffic CHannel)	Dedicated bidirectional channel used for the exchange of data with a mobile	Transparent, acknowledged or unacknowledged
CTCH (Common Traffic CHannel)	Common unidirectional channel used to send traffic data to a set of mobiles	Unacknowledged

Table 3.3. *The logical channels*

3.3.3. *MAC protocol*

The MAC layer carries out the following functions:

– connection of the logical channels with transport channels;

– selection of the appropriate format for each transport channel;

– priority management between the data flows at mobile level;

– priority management between several terminals;

– mobile identification on common channels;

– multiplexing and demultiplexing of RLC layer data units;

– the encryption of RLC data in transparent mode.

When multiplexing is not used, there is no MAC header (transparent mode). The transport channel is thus directly connected to a logical channel.

The DCH is used in the uplink and/or downlink. It transports the dedicated logical DCCH control and the DTCH (Dedicated Traffic CHannel).

Several common types of transport channel are used for the downlink (Figure 3.12):

– the BCH (Broadcast CHannel) is used to transmit system information (random access codes, available access slots, diversity method);

– the FACH is used to transmit control information to terminals in a given cell. It is also possible to transmit some traffic on the FACH;

– the PCH ensures the transmission of information necessary for the paging procedure;

– the DSCH (Downlink Shared CHannel) allows for the transmission of traffic data dedicated to a user on a channel shared by several users. It is similar to the FACH.

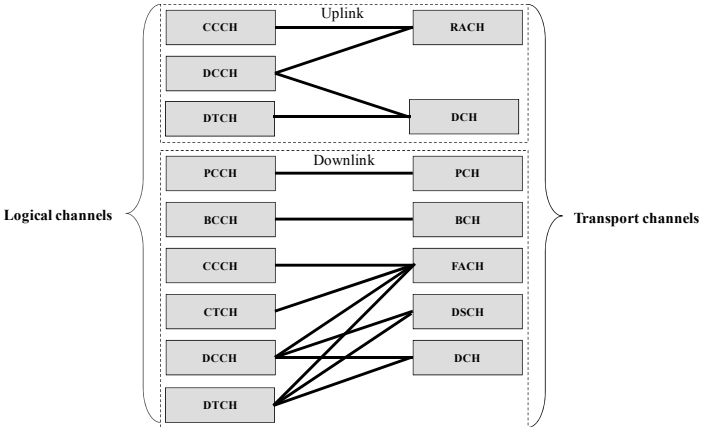


Figure 3.12. *Correspondence between the logical channels and the transport channels*

For the uplink, the common transport channels used are the shared CPCH (Common Packet CHannel) and the RACH (Random Access CHannel). The RACH is used to transmit control information, such as the connection establishment request. The CPCH is an extension of the RACH that is used to transmit user data. It is the FACH for the downlink (Figure 3.12).

The transport channel defines how information must be transmitted on the radio channel:

– the list of attributes associated with each transport format set channel;

– the size of the elementary data block TBS (Transport Block Size);

– the duration for the transmission of a transport block TTI (Transmission Time Interval);

– the type of channel coding (convolutional code, turbo code) and its rate;

– the size of the CRC (Cyclic Redundancy Check).

Table 3.4 contains the attributes of the DCH transport channel supporting the AMR coded channel.

Transport channels	**DCH (1)**	**DCH (2)**	**DCH (3)**	**DCH (4)**
TBS	81	103	60	148
TTI	20	20	20	40
CRC	12	0	0	16
Channel coding	1/3 Convolutional	1/3 Convolutional	1/2 Convolutional	1/3 Convolutional

Table 3.4. *The attributes of the AMR codec*

Table 3.5 contains the attributes of other transport channels.

Transport channels	**BCH**	**PCH**	**FACH, DCH, DSCH**	**RACH**
TBS	246	1 to 200,000	0 to 200,000	0 to 200,000
TTI	20	10	10, 20, 40, 80	10, 20
Channel coding	Convolutional	Convolutional	Turbo code	Convolutional
Coding rate	1/2	1/2	1, 1/2, 1/3	1/2
Size of the CRC	16	0, 8, 12, 16, 24	0, 8, 12, 16, 24	0, 8, 12, 16, 24

Table 3.5. *The attributes of the transport channels*

The structure of the MAC header depends on the type of logical channel used and on the use of the multiplexing function of several logical channels or several users. The MAC header contains the following fields (Figure 3.13):

– TCTF (Target Channel Type Field): this field provides the type of logical channel transported in the transport channel;

– UE-Id Type: this field indicates the user's identification type;

– U-RNTI (UTRAN Radio Network Temporary Identity);

– C-RNTI (Cell Radio Network Temporary Identity);

– UE-Id: this field provides the user's identification;

– C/T: this field provides the user's logical channel number.

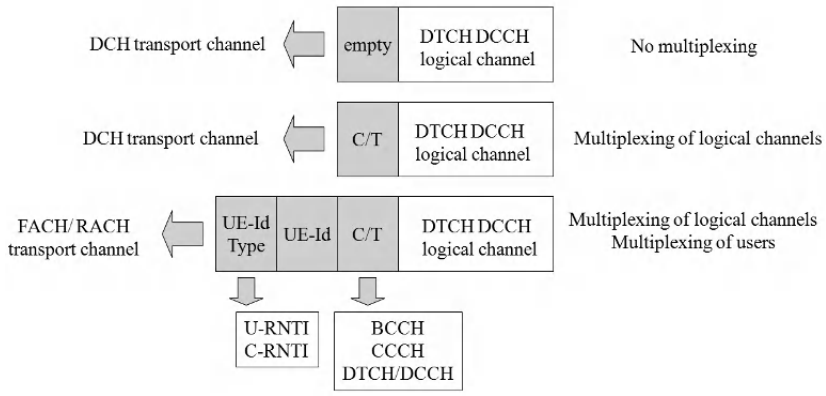


Figure 3.13. *The structure of the MAC header*

3.3.4. *Physical layer*

The transmission chain of the physical layer consists of the following functions (Figure 3.14):

– channel coding and multiplexing;

– transition of the bit to the symbol;

– spread spectrum;

– radio frequency modulation.

The reception chain of the physical layer has the following functions (Figure 3.14):

– radio frequency demodulation;

– despread spectrum;

– detection with a RAKE receiver;

– demultiplexing and decoding of the channel.

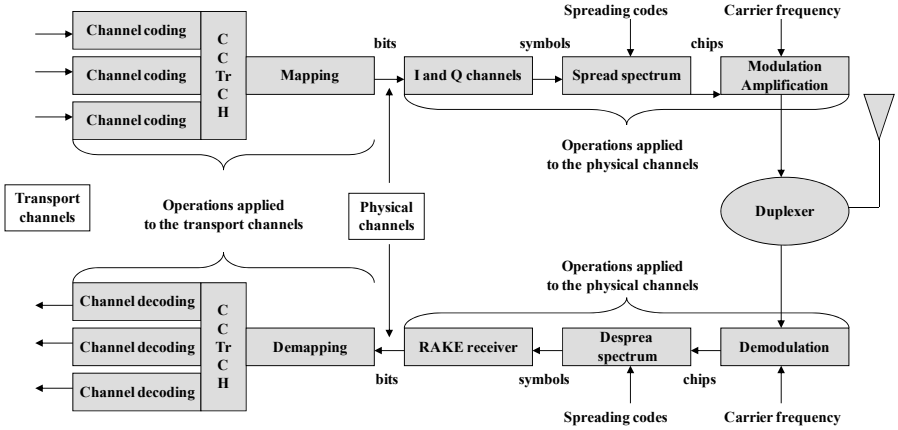


Figure 3.14. *The transmission chain*

3.3.4.1. *Physical channels*

The data generated by the MAC layer are transmitted across the radio interface on different physical channels (Figure 3.15). The physical layer must be able to support different rates in order to offer bandwidth services upon request and multiplex several services on the same connection.

Each transport channel receives a transport format indicator each time data arrives from the MAC layer. The physical layer combines the information contained in the transport format indicators from different transport channels into a new TFCI (Transport Format Combination Indicator). The TFCI is transmitted across the physical control channel in order to inform the receiver of the active transport channels.

This is in addition to the physical channel, which only transports information belonging to the procedures of the physical layer. These channels ensure the synchronization functions (SCH or Synchronization CHannel and CPICH or Common PIlot CHannel), the access control function for the common channels of the uplink (AICH or Acquisition Indicator CHannel), and the mobile's call-waiting function (PICH or Paging Indicator CHannel).

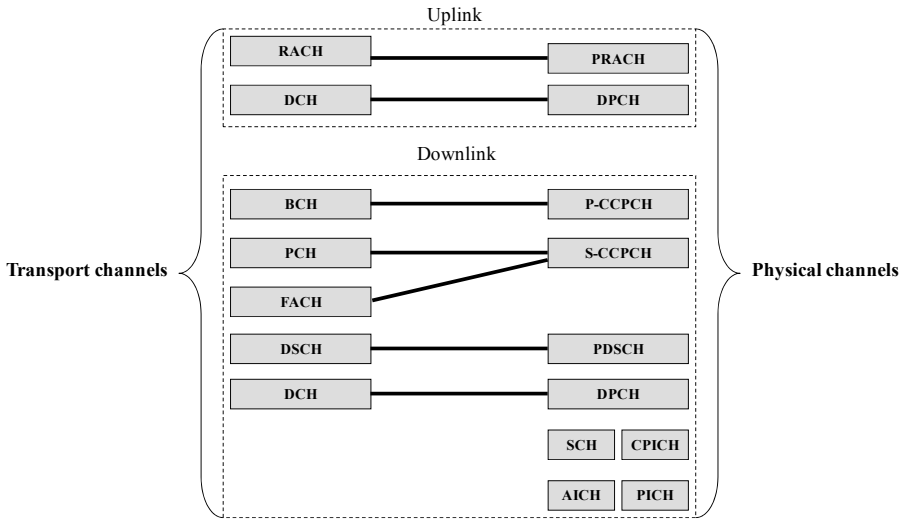


Figure 3.15. *Correspondence between the transport and physical channels*

3.3.4.2. *The multiplexing of transport channels*

Channel coding is carried out individually on each transport channel. After receiving a transport block from the MAC layer, the first operation is to add a CRC to detect errors at receiver level. The length of the CRC code is 0, 8, 12, 16 or 24 bits. The second operation is to apply a convolutional code to the coded blocks. Rate adaptation is used to change the number of bits to be transmitted to the number of bits available in the frame. This is achieved by puncturing or repetition (Figure 3.16).

The segmentation function is used to guarantee that the data are divided into blocks of equal size when they must be transmitted on more than one frame of 10 ms.

The first inter-frame interleaver is achieved on two, four, six or eight frames.

The different transport channels are multiplexed to create a single coded composite transport channel) that will then be mapped on a physical channel.

The second operation of the intra-frame interleaver is carried out and then the signal is mapped on the slots of the physical channel.

The physical channels use a 10 ms (i.e. 38,400 chips) radio-frame structure, each frame being cut into 15 slots of 66.7 μs (i.e. 2,560 chips).

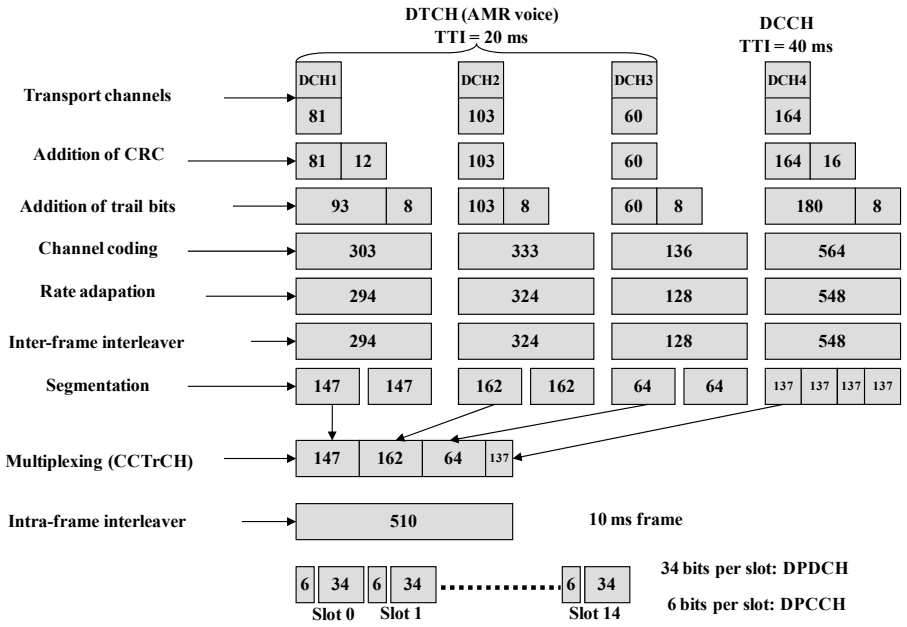


Figure 3.16. *The multiplexing of transport channels*

3.3.4.3. *Traffic channels*

The DPCH (Dedicated Physical CHannel) is a resource appointed to a user that offers a constant rate. It consists of two physical sub-channels (Figure 3.17):

– the DPDCH (Dedicated Physical Data CHannel) transmits the data from the user plane and signaling exchanged between the mobile and the RNC, MSC or SGSN;

– the DPCCH (Dedicated Physical Control CHannel) transmits specific control data from the physical layer, containing:

- the pilot bits for estimation of the impulse response of the channel;

- the transmit power control bits for power control;

- the TFCI bits in order to indicate the format of the transport channel;

- the FBI (FeedBack Indicator) bits in the uplink, which are used when there is diversity in emission.

The multiplexing of DPDCH and DPCCH sub-channels is different for both transmission directions. Each sub-channel is separated on the I and Q channels for the upstream channel. The multiplexing is a time-division for the downlink.

For the uplink, the DPCCH control channel is transmitted with a fixed spreading code of 256. The DPDCH uses a variable spreading factor (SF) of between four and 256. The rate of the DPDCH channel can vary from frame-to-frame, the rate being indicated on the DPCCH by the TFCI.

For the downlink, the SF used for the rate corresponding to the multiplexing of the Dedicated Physical Control and Dedicated Physical Data sub-channels determines the channelization code, which can vary from 4 to 512. This method is used to minimize channelization code consumption.

The downstream channel can use two modes of transmission diversity in order to improve the radio transmission performance. Open-loop transmission diversity consists of sending the information on two antennas. Closed-loop diversity consists of using the FBI bits received from the mobile to adjust the signals transmitted by Node B in phase and in amplitude.

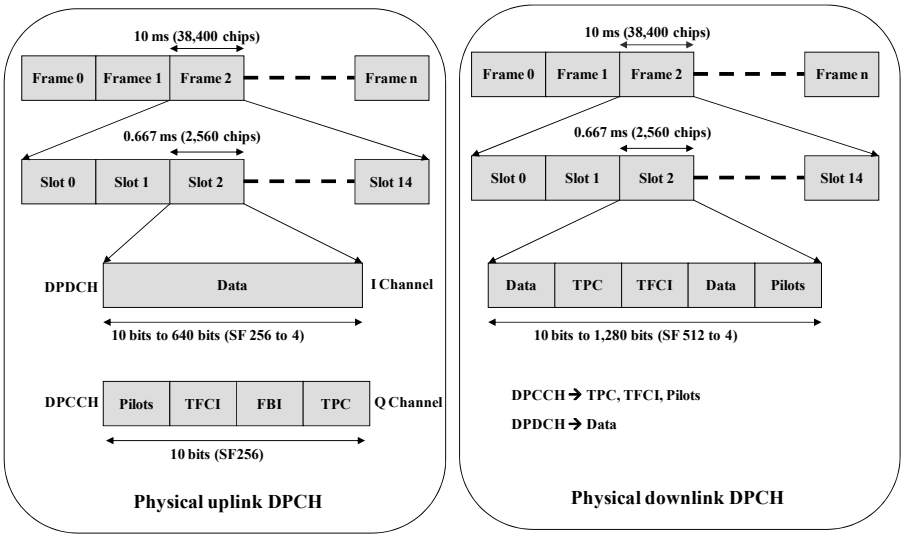


Figure 3.17. *The structure of the DPCH*

The PDSCH (Physical Downlink Shared CHannel) channel transports the binary elements of the DSCH transport channel in the downlink. It is shared by several users following code-division multiplexing. The PDSCH does not contain control information about the physical layer; this is transmitted by a specific DPCH.

3.3.4.4. *Control channels*

3.3.4.4.1. The SCH

The SCH consists of two channels: the primary SCH (P-SCH) and the secondary SCH (S-SCH).

The primary SCH P-SCH uses a spreading sequence of 256 chips that are identical for each cell. This sequence is transmitted to each slot. It is used to carry out receiving synchronization at slot level and for selection of the signal allocated to the RAKE receiver. The P-SCH does not support the transport channel (Figure 3.18).

The S-SCH is a series of 15 spreading sequences of 256 chips, constituting one group in 64 possible groups. The sequences of the S-SCH are transmitted in synchronization with the P-SCH. The S-SCH is used when receiving in order to apply frame synchronization and identify the cell in a given geographical area. The S-SCH does not support transport channels (Figure 3.18).

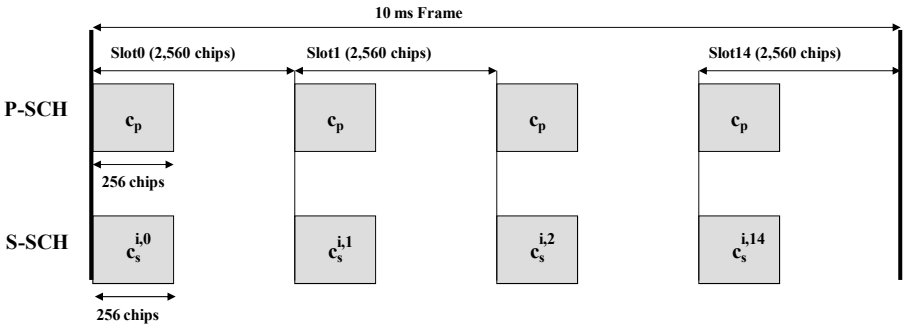


Figure 3.18. *Transmission of the SCH*

3.3.4.4.2. The CPICH

The CPICH has 10 symbols (or 20 bits) per slot. It is coded with a channelization code with a SF of 256 (C0,256) and with a primary scrambling code specific to the cell. There are 512 scrambling codes, organized into 64 groups of eight codes. The group is obtained from the S-SCH channel. When it has obtained the group, the mobile must find the scrambling code of the cell (one out of eight). The CPICH does not support transport channels (Figure 3.19).

The CPICH is used by mobiles to carry out power measurements in the current cell and in the neighboring cells, and to estimate the impulse response of the RAKE receiver.

When the CPICH intervenes in transmit diversity, it is transmitted on two antennas with the same channelization and scrambling code, but with different symbols.

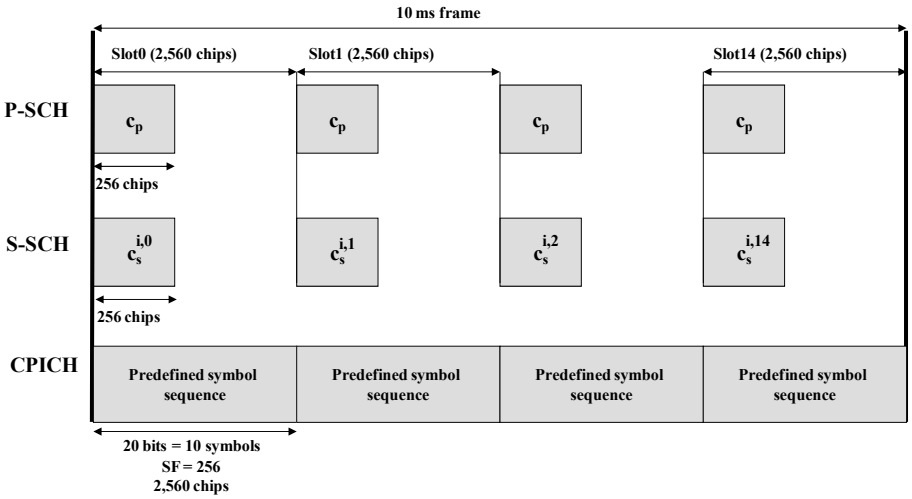


Figure 3.19. *The transmission of the CPICH*

3.3.4.4.3. The P-CCPCH

The P-CCPCH (Primary Common Control Physical Channel) transports the BCH. It consists of a continuous rate of nine symbols per slot, with a channelization code of a SF of 256 (C1, 256). The channel is protected by a half rate convolutional code. The P-CCPCH is alternately transmitted with the SCH. It is possible to apply a method of transmit diversity (Figure 3.20).

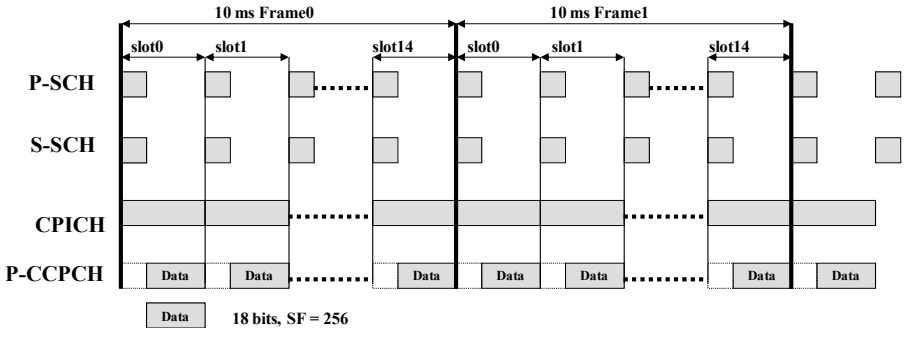


Figure 3.20. *The transmission of the P-CCPCH*

3.3.4.4.4. The S-CCPCH and PICH

The S-CCPCH (Secondary Common Control Physical Channel) transports the FACH and PCH on the downlink. Both the FACH and PCH can be multiplexed on the same S-CCPCH or use two distinct physical channels. The SF of the S-CCPCH can vary from 4 to 256. The S-CCPCH can also use the transmit diversity method (Figure 3.21).

The S-CCPCH contains three types of information:

– data bits from signaling messages;

– physical layer control bits (pilot bits) allowing for an estimation of the channel's impulse response;

– TFCI bits provide the format for the transport channel contained in the current frame.

The PICH functions in conjunction with the S-CCPCH in order to ensure that the mobile works sufficiently in idle mode. The paging indicators use a channelization code at a length of 256 chips and are transmitted once per slot onto the PICH. Each PICH frame of 10 ms transports 288 bits corresponding to18, 36, 72 or 144 paging indicators. When in the frame, the paging indicator is placed at 1, this indicates that the mobile concerned must read the S-CCPCH frame (Figure 3.21).

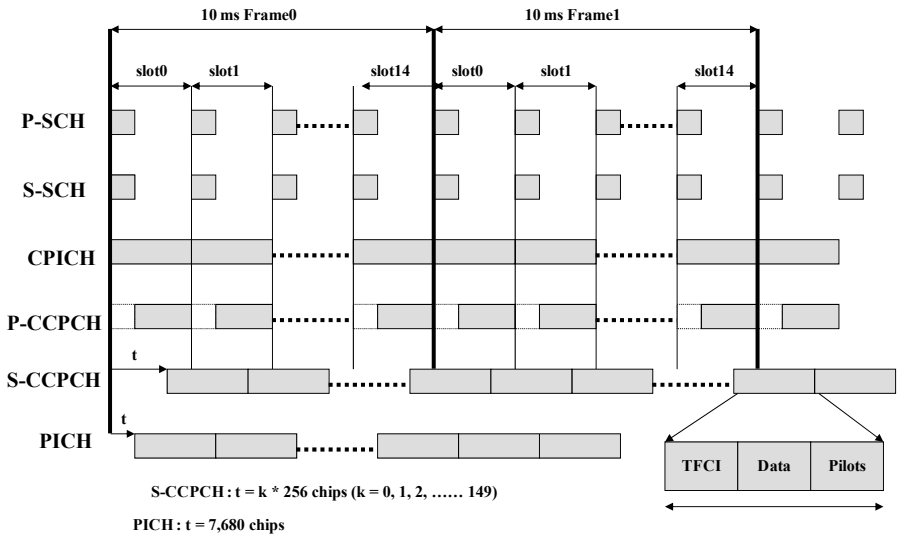


Figure 3.21. *The transmission of the S-CCPCH and PICH*

3.3.4.4.5. The PRACH and AICH

The PRACH (Physical Random Access CHannel) transports the RACH, allowing mobiles to access the network. It sets up a random access method on the uplink. It is used for signaling during registration of the mobile, during a location update procedure, and for the transmission of small packets of information (Figure 3.22).

The structure of the PRACH is the same as the channel used to transport traffic data. The rate must be maintained at a value that is low enough to avoid limiting radio coverage.

The PRACH uses an open-loop power control. The power level of the downlink is measured, defining the initial level of power transmitted. A preamble of 4,096 chips is sent with a spreading code equal to 256.

The mobile decodes the AICH in order to be assured that Node B has received the preamble. When the preamble is not detected, the terminal increases the power transmitted until acknowledged by the network. When the mobile has received a response from Node B, it transmits data over a duration of 10 or 20 ms, with a spreading code from 32 to 256, with a half rate convolutional code (Figure 3.22).

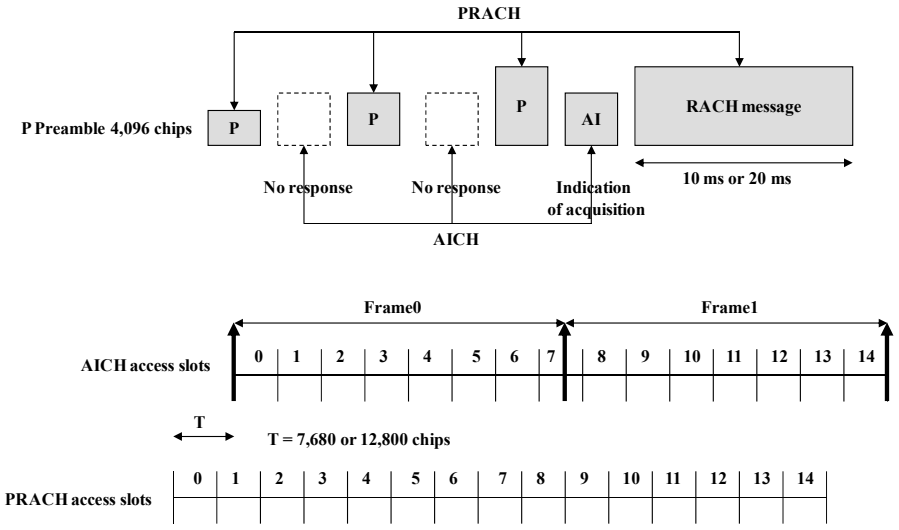


Figure 3.22. *Transmission of the PRACH and AICH*

Mobile transmission is distributed into 15 windows every 20 ms. The mobile randomly chooses one of the available signatures and its connected channelization code. The signatures available in the cell are broadcast on the BCCH.

The AICH is transmitted by Node B to indicate that the signature sequence of the RACH has been received. The structure of the AICH is the same as that used by the PRACH preamble. The AICH does not support transport channels. It is directly controlled by the physical layer (Figure 3.22).

3.3.5. *The spread spectrum*

The mobile uses a multiple access mode by CDMA (Code Division Multiple Access) code allocation. The user data are spread over a large bandwidth by multiplying them via a pseudo-random sequence (or spreading code) of bits (called chips) at a higher rate (3.84 Mc/s). The chip rate of 3.84 Mc/s gives a bandwidth via the carrier in the region of 5 MHz.

The CDMA system is used to multiplex several users at the same time and on the same frequency. At Node B level, upon reception users are distinguished from the correlation properties of scrambling codes. The spread method consists of multiplying each bit of the initial data by a sequence of *n* chips. Despreading consists of multiplying signal spread by the same code. When despreading is applied to another sequence, the result of the multiplication and its integration gives a value close to zero (Figure 3.23).

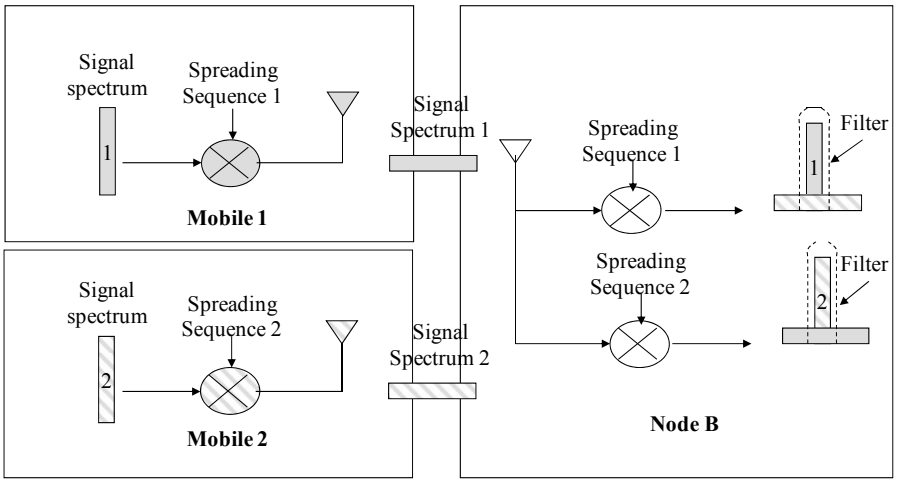


Figure 3.23. *The principals of spreading*

The signals transmitted by the same source are separated via channelization codes. For the downlink, the signals are bound for different mobiles connected to Node B. For the uplink, the different signals come from different flows generated by the mobile.

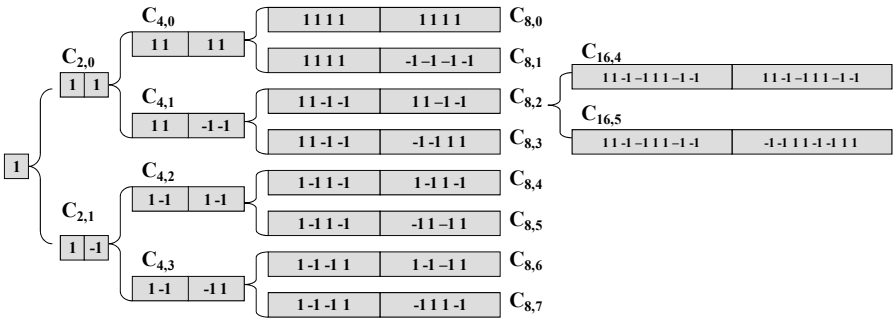


Figure 3.24. *The channelization code*

The Walsh-Hadamard channelization codes have the advantage of being orthogonal in certain conditions. Two sequences located at the same hierarchical level are orthogonal. Two sequences located on the same tree are not orthogonal. They are a rare resource shared by all mobiles in the downlink, whose allocation is managed by the RNC (Figure 3.24).

The length of the SF code varies between 4 and 512 chips in the downlink and from 4 to 256 in the uplink. It determines the available rate of the DPDCH (Table 3.6).

Channel	Spreading factor	Rate in kbps
Upstream channel	4	960
	256	7.5
Downstream channel	4	1920
	512	7.5

Table 3.6. *The rates of the DPDCH*

The channelization codes are not pseudo-random sequences and they do not necessarily carry out a spread spectrum. Furthermore, orthogonality is obtained solely for synchronized sequences, from where there is difficulty for the uplink where the mobiles are not synchronous.

The introduction of a second spreading code, the scrambling code, allows for the separation of between sources (sectors in the downlink, mobiles in the uplink). The gold scrambling codes have good autocorrelation and intercorrelation properties, and a large number of codes can be generated. On the other hand the scrambling codes are not orthogonal to each other (Figure 3.25).

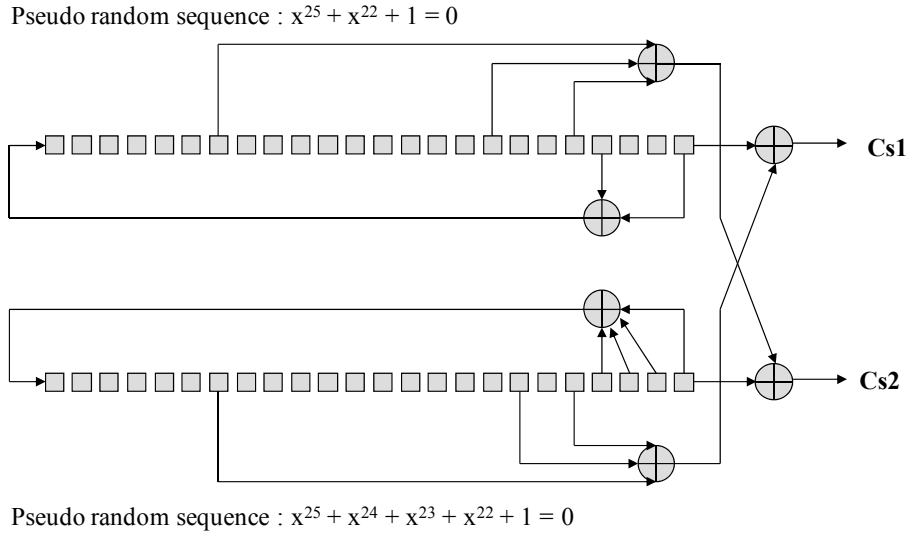


Figure 3.25. *The scrambling code*

3.3.6. *Modulation*

For the downlink, the QPSK (Quadrature Phase Shift Keying) modulation is applied with time-divisionally multiplexed DPDCH data and DPCCH control flows (Figure 3.26).

For the uplink, neither the DPDCH nor the DPCCH is time-divisionally multiplexed. Multiplexing is achieved at complex scrambling level (Figure 3.26).

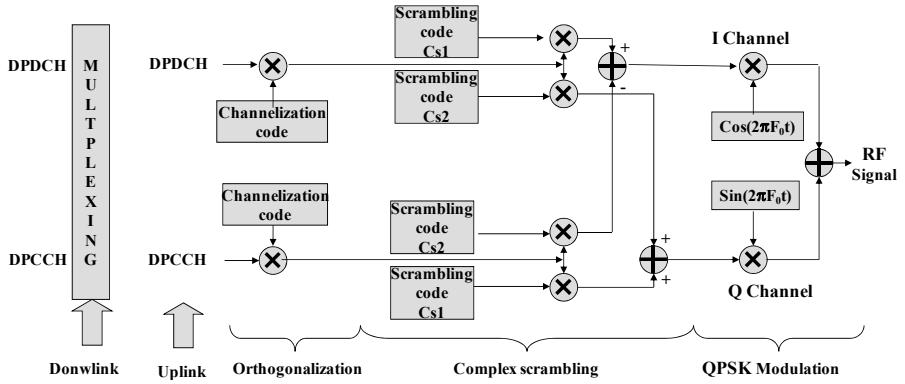


Figure 3.26. *Modulation*

3.3.7. *The frequency plan*

The CDMA system possesses two modes:

– the FDD (Frequency Duplex Division) mode. Two bandwidths of 5 MHz are used − one for the uplink, the other for the downlink − spaced at 190 MHz;

– the time duplex division mode: s single bandwidth of 5 MHz is used for both transmission directions[3].

The frequency band reserved for the UMTS is divided into several sub-bands according to the mode (Figure 3.27):

– 1,920–1,980 MHz for the uplink of the FDD mode;

– 2,110–2,170 MHz for the downlink of the FDD mode;

– 1,900–1,920 MHz and 2,010-2,025 MHz for the time duplex division mode.

In the GSM, the planning consists of allocating a frequency band to each cell from a frequency reuse pattern. One cell can consume several frequencies in the case of high density.

In the UMTS, the same frequency is used for each cell. The reuse pattern is based on two codes, which makes the operation simpler:

– the secondary synchronization channel code;

– the primary scrambling code.

3 The time duplex division mode is not covered.

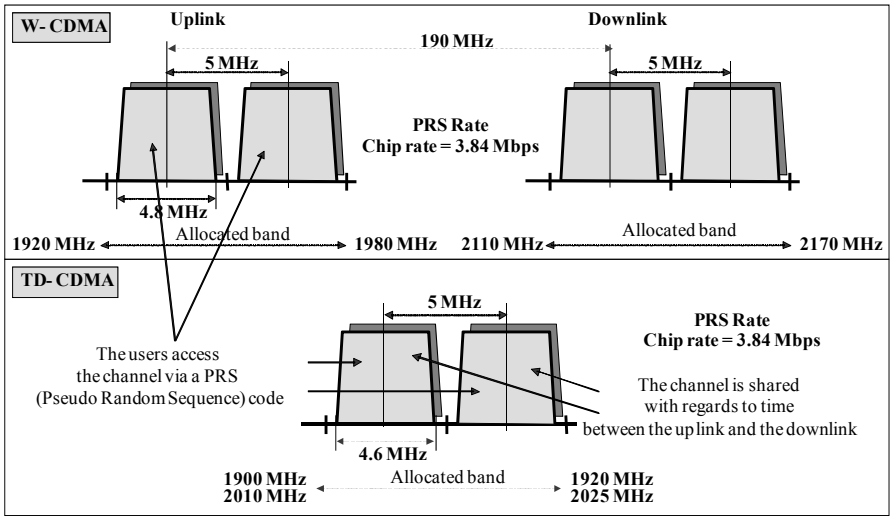


Figure 3.27. *The frequency plan*

3.3.8. *Power control*

Power control is the most important aspect of the CDMA system, especially at uplink level. Without this function, a mobile transmitting a power level that is too strong can stop all other mobiles from communicating.

In the absence of power control, a mobile signal located along the cell is received with an amplitude that is much smaller than that of the mobile located close to Node B. Like mobiles transmit at the same time and on the same frequency and the signals can only be distinguished by their code. The gain generated by the intercorrelation of the codes can prove insufficient to compensate for the power difference.

The closed-loop fast control (closed-loop power control) is a mechanism that allows for adjustment of the power emitted by the mobiles in order to guarantee a constant level when receiving. Node B carries out estimations of the SIR (signal to interference ratio) and compares them to a target value. If the estimated SIR is above the target value, node B requests that the mobile reduce its transmission power. In the opposite case, the mobile will be requested to increase its transmission power. This operation is carried out 1,500 times a second (Figure 3.28).

The outer loop power control is a mechanism that allows for the adjustment of the target value of the SIR according to error rate. The target value of the SIR is not a constant and can vary according to the speed of the mobile and the multipath

profile. For each frame received from the mobile, Node B adds a quality indicator that will inform the RNC of deterioration in transmission. The RNC will command Node B to increase the value of the target SIR (Figure 3.28).

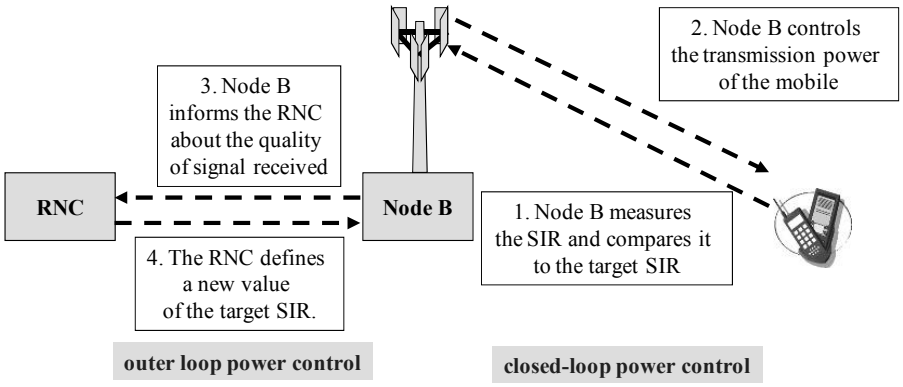


Figure 3.28. *The power control*

3.3.9. *The RAKE receiver*

Radio propagation is characterized by multiple reflections caused by natural obstacles. The signal can be received several times, with a stronger or weaker power. The signal can add more or less time in order to arrive at the receiver. The variation in propagation time is in the region of 2 μs in an urban environment and 20 μs in a rural environment. This propagation time variation between two received signals is above the duration of a chip (0.26 μs). This allows the receiver to identify the different signals received, separate them and combine them in a coherent manner. The minimum period of 0.26 μs corresponds to a path difference of 78 m.

The RAKE receiver allocates a correlation receiver (a finger of the receiver) to each signal during time-slots when a significant part of the signal arrives at the receiver. This function is achieved by a matched filter that allows the delay profile due to the multipath to be defined (Figure 3.29).

At each finger, the code generator and the correlator perform the task of despreading and user signal integration. The module dedicated to the estimation of the channel uses a pilot signal to evaluate the transfer function of the radio channel. The delay between the arrival times of different signals is compensated for at the delay equalization module.

The last module of the processing chain, the combiner − which is shared by all fingers − carries out the summation of signals. This operation that brings a diversity of paths is used to fight against the signal fading.

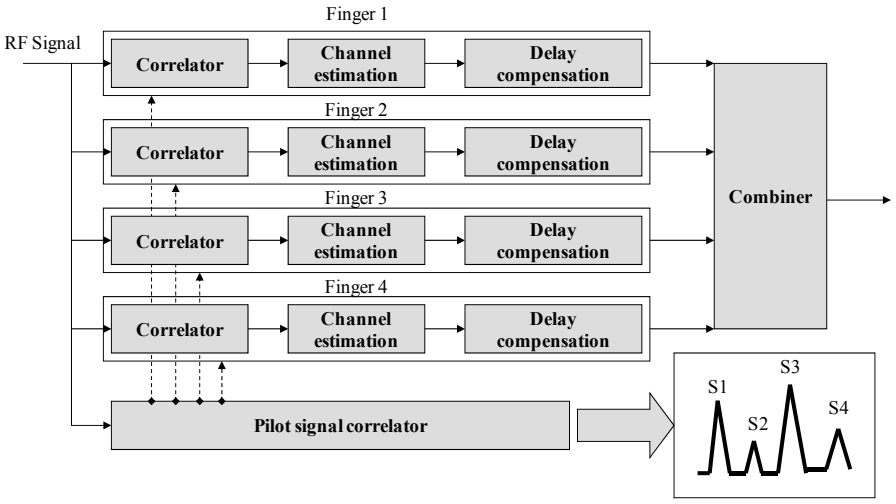


Figure 3.29. *The RAKE receiver*

3.4. Communication management

The procedures described concern the signaling protocols of the access stratum. The procedures concerning the signaling protocols of the NAS are similar to those described in the GSM and GPRS networks.

3.4.1. *The establishment of a connection for the NAS*

The establishment of a connection for NAS signaling is carried out at the initiative of the mobile or following a paging received from the NSS or GSS core network (Figure 3.30).

The mobile sends the RRC CONNECTION REQUEST message on the logical CCCH, mapped on the transport RACH. The RNC allocates the U-RNTI and C-RNTI and transmits the RRC CONNECTION SETUP message on the logical CCCH, mapped on the transport FACH. The mobile returns the RRC CONNEXION SETUP COMPLETE message on the logical DCCH mapped on the transport RACH.

The mobile sends the RRC INITIAL DIRECT TRANSFER message to the RNC on the logical channel, mapped on the transport RACH. The RNC initializes a signaling connection (SCCP procedure) with the core network and sends the RANAP INITIAL UE MESSAGE.

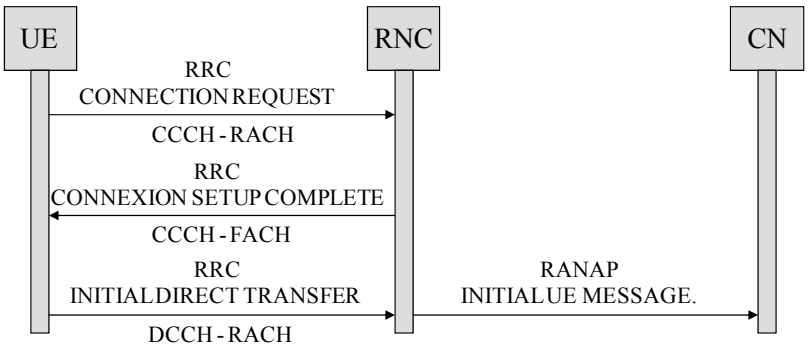


Figure 3.30. *The establishment phases of a connection for the NAS*

3.4.2. *Paging*

The mobile can receive a paging for CSs or PSs. As the mobile is in an idle mode (RRC Idle), its location is only known by the core network and consequently the paging is spread over a defined geographical area (Figure 3.31).

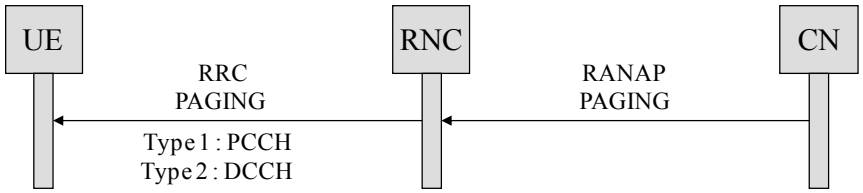


Figure 3.31. *The establishment phases of paging*

The core network launches paging via the RANAP PAGING message. Paging of the mobile uses the logical PCCH (type 1 paging). The mobile detects the message from the RNC and starts the NAS signaling procedure.

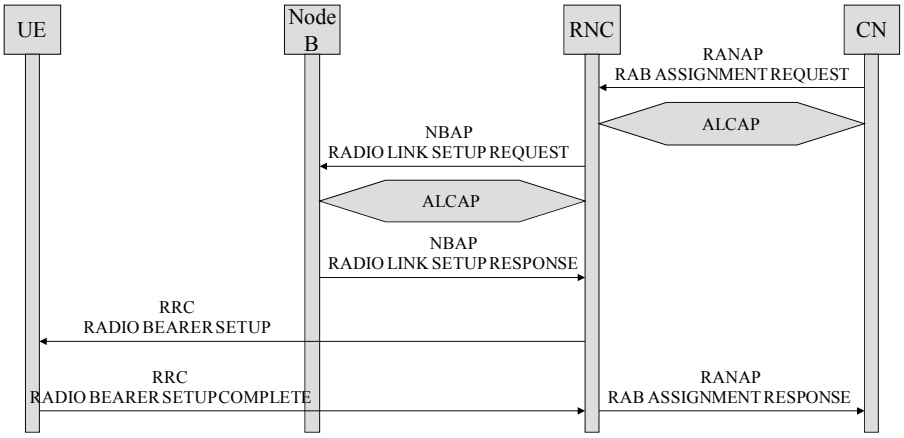
This operating mode also applies when the mobile is connected, in the CELL_PCH and URA_PCH states.

When the mobile is connected in the CELL_DCH and CELL_FACH states, the access UTRAN integrates the paging with the existing connection with the help of the logical DCCH (type 2 paging).

3.4.3. *Establishment of the RAB*

The core network initializes the establishment of the RAB with the RANAP RAB ASSIGNMENT REQUEST message (Figure 3.32).

The RNC initializes the establishment of the resource on the Iu interface via the ALCAP (Access Link Control Application Part) protocol, transmits the NBAP RADIO LINK SETUP REQUEST message to Node B and initializes establishment of the resource on the Iub interface.



CN – Core Network

Figure 3.32. *Establishment phases of the RAB*

Node B reserves the resource on the radio interface and responds to the RNC with the NBAP RADIO LINK SETUP RESPONSE message.

The RNC sends the RRC RADIO BEARER SETUP message to the mobile on the logical DCCH, which is acknowledged in return by the RRC RADIO BEARER SETUP COMPLETE message. The RNC acknowledges the establishment of the RAB by transmitting the RANAP RAB ASSIGNMENT RESPONSE message to the core network.

3.4.4. *Soft handover*

The soft handover allows the mobile to be simultaneously connected to several B Nodes, which are connected to different RNCs. The SRNC is that which initialized the establishment of the connection. The DRNC is used to establish a link between the Node B that it controls and the SRNC (Figure 3.33).

The SRNC decides to establish a link with a new Node B controlled by another RNC. It transmits a RNSAP RADIO LINK SETUP REQUEST message to the DRNC.

The DRNC implements the establishment of the RAB with Node B and sends a confirmation to the SRNC with the RNSAP RADIO LINK SETUP RESPONSE message.

The SRNC transmits the RRC ACTIVE SET UPDATE message to the mobile on the logical DCCH to notify it of the establishment of a new radio link. This is acknowledged in return by the RRC ACTIVE SET UPDATE COMPLETE message.

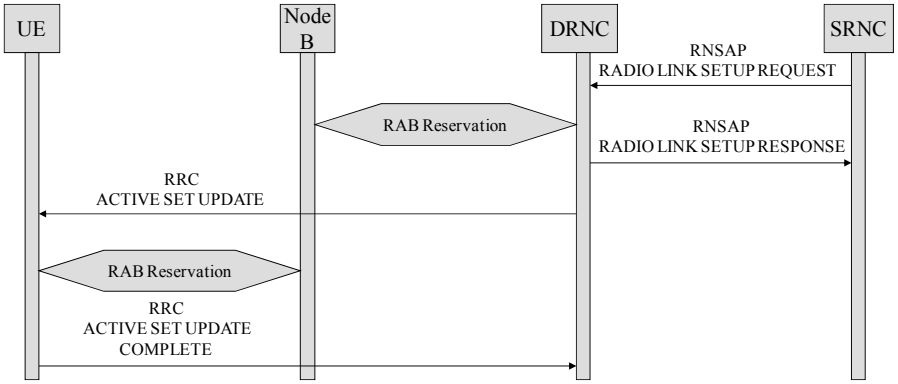


Figure 3.33. *The establishment phases of the soft handover*

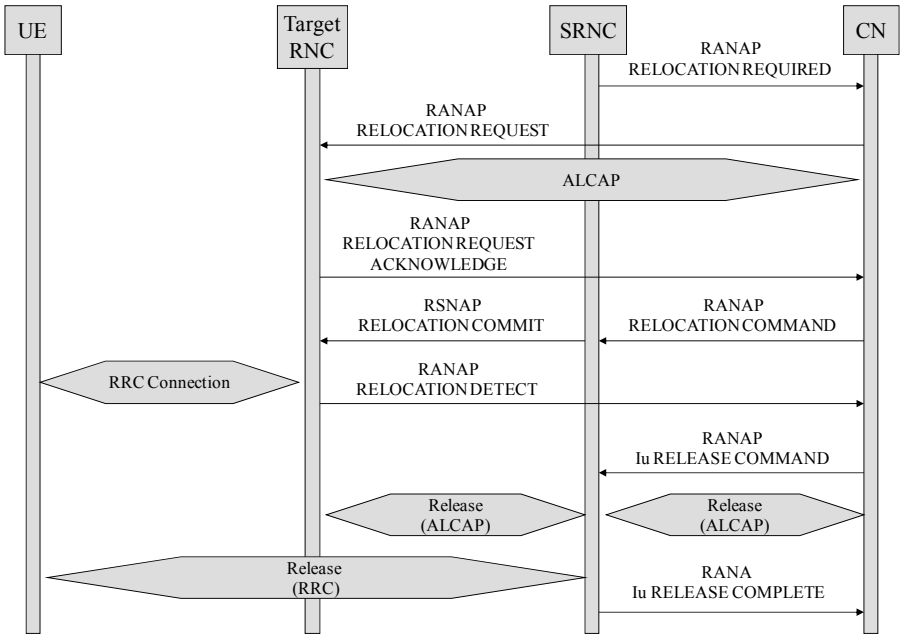
3.4.5. *Relocation*

The relocation procedure is used to modify the anchor point of the mobile. It leads to a change in the current SRNC in order to optimize data transfer in the access UTRAN or with a hard handover (Figure 3.34).

The SRNC transmits the RANAP RELOCATION REQUIRED message to the core network.

The core network transmits the RANAP RELOCATION REQUEST message to the target RNC in order to reserve the resources on the Iu interface. The target RNC responds to the core network with the RANAP RELOCATION REQUEST ACKNOWLEDGE message.

The core network indicates the completion of the relocation preparation phase to the SRNC by sending the RANAP RELOCATION COMMAND message. The SRNC sends the RSNAP RELOCATION COMMIT message to the target RNC in order to proceed to the execution of the relocation.



CN – Core Network

Figure 3.34. *The establishment phases of relocation*

The target RNC sends the RANAP RELOCATION DETECT message to the core network and proceeds to connect with the mobile. When connnection is established, it sends the RANAP RELOCATION COMPLETE message.

The core network initializes the release of resources with the SRNC by sending the RANAP Iu RELEASE COMMAND message. The SRNC releases the resources allocated to the mobile and responds with the RANAP Iu RELEASE COMPLETE message.

3.4.6. *Inter-system handover*

3.4.6.1. *Handover from the UMTS to the GSM*

When the mobile is on the UMTS network, transmission is continuous. In order to receive the information transmitted by the GSM network, the mobile must switch to compressed mode. The idea is to create free spaces with duration of several time-slots per frame.

Several methods have been defined in order to compress the data transmitted on the radio interface:

– puncturing: after applying the channel coding (convolutional or turbo code), a certain number of bits are deleted, which reduces redundancy and increases awareness of transmission errors;

– reduction of the SF: the frame is transmitted with a halved SF, which reduces the gain connected with spreading;

– use of a transport format that reduces the number of bits per frame.

Based on measurements carried out by the mobile, the SRNC takes control of the handover and transmits the RANAP RELOCATION REQUIRED message to the MSC 3G, which provokes the initialization of the inter-MSC handover procedure with the MSC 2G of the GSM network (Figure 3.35).

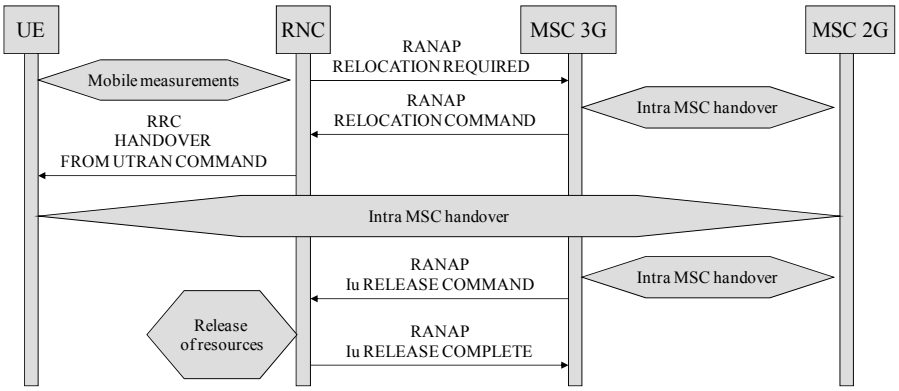


Figure 3.35. *The establishment phases of the handover from the UMTS to the GSM*

If the resources are available in the GSM network, the MSC 3G starts the relocation procedure by transmitting the RANAP RELOCATION COMMAND message to the SRNC.

The SRNC provokes the handover at mobile level by sending it the RRC HANDOVER FROM UTRAN COMMAND message.

When the handover procedure has been carried out in the GSM network, the MSC 3G initializes the release of resources with the SRNC by sending the RANAP Iu RELEASE COMMAND message. The SRNC releases the resources allocated to the mobile and responds with the RANAP Iu RELEASE COMPLETE message.

3.4.6.2. *Handover from the GSM to the UMTS*

After the handover request from the MSC 2G is received, the MSC 3G sends the RANAP RELOCATION REQUEST message to the target RNC. In response, the RANAP RELOCATION REQUEST ACKNOWLEDGE message provokes the handover at mobile level (Figure 3.36).

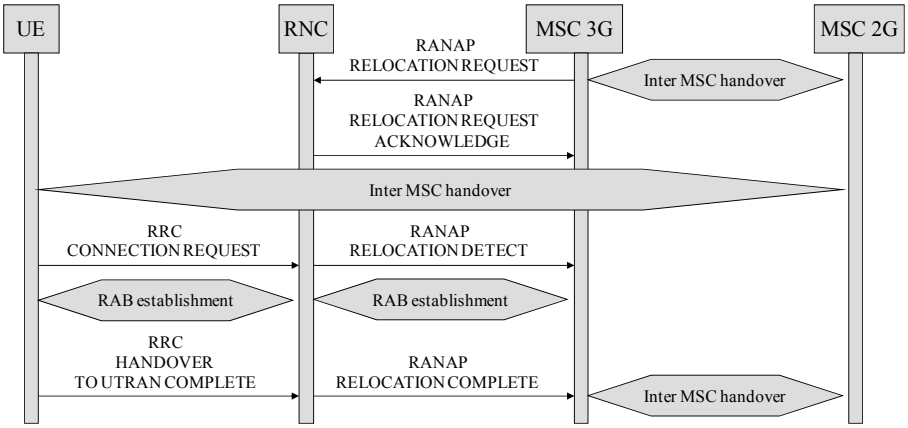


Figure 3.36. *The establishment phases of handover from the GSM to the UMTS*

When the RNC has detected the mobile, it sends a RANAP RELOCATION DETECT message to the MSC 3G. When the RRC connection is established with the target RNC and the necessary radio resources are allocated, the mobile sends the RRC HANDOVER TO UTRAN COMPLETE message. The RNC confirms handover to the MSC 3G by sending the RANAP RELOCATION COMPLETE message, which then provokes the release of resources from the GSM network.

3.5. HSPA evolutions

3.5.1. *The HSDPA evolution*

The HSDPA (High Speed Downlink Packet Access) evolution is used to increase the rate in the downlink by aggregating the channels and increasing the number of bits per symbol for the modulation. The downlink resource is shared between the different mobiles. The following functions are available (Table 3.7):

– adaptation to the radio transmission conditions is carried out by selecting an appropriate combination of codes, the coding rate (from R = 1 / 3 to R = 1) and a type of modulation; QPSK or 16-QAM (Quadrature Amplitude Modulation);

– resource allocation is carried out for a TTI frame of 2 ms, with a fast signal at physical layer level;

– retransmission in the case of error or loss is carried out at physical layer level;

– the use of several codes with a single SF (SF=16) is used to increase the resource shared between mobiles.

Functions	UMTS	HSDPA
Variable spreading factor	Yes, the value is between 4 and 512 for the downlink; 4 and 256 for the uplink	No, the value is fixed and equal to 16
Fast power control	Yes	No
Adaptive modulation and coding	No	Yes
Multi-code operation	Yes, but rarely used	Yes, 15 SF16 codes can be used simultaneously
Retransmission at physical layer level	No the retransmission is ensured by the RLC layer	Yes retransmission is also ensured by the RLC layer, if it fails at physical layer level
Node B scheduling	No	Yes
Soft handover	yes	No
Duration of the frame in ms	80, 40, 20, 10	2

Table 3.7. *The UMTS and HSDPA functions*

3.5.1.1. *The MAC layer*

The MAC UMTS frames transmitted by the RNC are encapsulated at Node B level by a MAC-hs header, to create the HS-DSCH (High-Speed Downlink Shared CHannel).

An important property of the HS-DSCH is the dynamic nature of resource sharing for the TTI allocation period of 2 ms. When there are data for a user, they are streamed. There is no discontinuous transmission as with the DCH, as this reduces the interference of the downlink channel. If there are no longer any data to transmit to a mobile, the resource for the 2 ms is allocated to another user.

The MAC-hs header contains the following fields (Figure 3.37):

– VF (Version Flag): this field allows for future extension of the protocol;

– Queue ID: this field allows for identification of the reorganization queue at mobile level;

– TSN (Transmission Sequence Number): this field provides a SN used for the reorganization of data during retransmission;

– SID (Size Index identifier): this field identifies the size of the MAC UMTS frame. The RLC frame can take two values: 320 or 640 bits;

– N: this field provides the number of MAC frames which have the same length;

– F (Flag): this field is a flag that indicates whether the following field is an SID field.

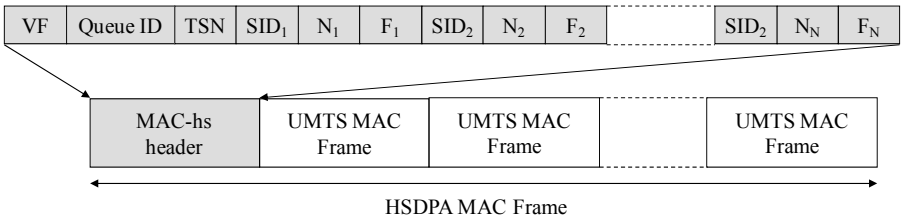


Figure 3.37. *The structure of the MAC-hs header*

3.5.1.2. *The physical layer*

The HS-PDSCH (High-Speed Physical Downlink Shared CHannel) is used to support the HS-DSCH transport channel. It corresponds to a channelization code with a spreading factor equal to 16, which allows for a rate of 960 kbps with a 16-QAM modulation. It is possible to aggregate up to 15 codes, in order to obtain a rate of 14.4 Mbps.

The HS-SCCH (High-Speed Shared Control Channel) is used in the downlink to transport control data by allowing HS-PDSCH processing. Two time-slots (2 × 2/3 ms) are transmitted before the that of the physical HS-PDSCH, so that the mobile has the information to process the latter (Figure 3.38).

The first part is transmitted in the first time-slot of the 2 ms frame and transports the critical information in the time needed to trigger the demodulation process on time. The parameters of the first part indicate the codes to despread and the type of modulation used − QPSK or 16-QAM.

The second part is transmitted in the two other time-slots that contain parameters less sensitive to time, such as which HARQ (Hybrid Automatic Repeat-reQuest) retransmission mechanism to use.

The type I HARQ mechanism or soft combining is characterized by retransmission of the same data block. The type II HARQ mechanism uses the principals of incremental redundancy, where each retransmission corresponds to a different puncturing scheme.

When the principal of time-division multiplexing is used, a single HS-SCCH is configured, and in this instance a single user receives data. When the principal of code-division multiplexing is used, several HS-SCCHs must be involved. A mobile must be able to deal with four HS-SCCHs simultaneously.

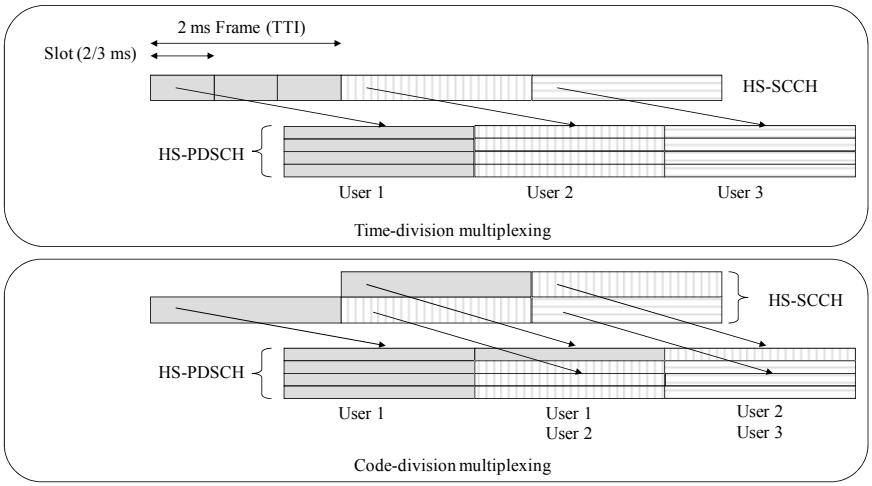


Figure 3.38. *The transmission of the HS-DPDSCHs and HS-SCCHs*

The HS-DPCCH (High-Speed Dedicated Physical Control CHannel) is used in the uplink to transport the following control data (Figure 3.39):

– HARQ: this field indicates whether the data received are correct or erroneous;

– CQI (Channel Quality Information): this field indicates a level corresponding to characteristics of radio propagation, to determine the rate the mobile can receive.

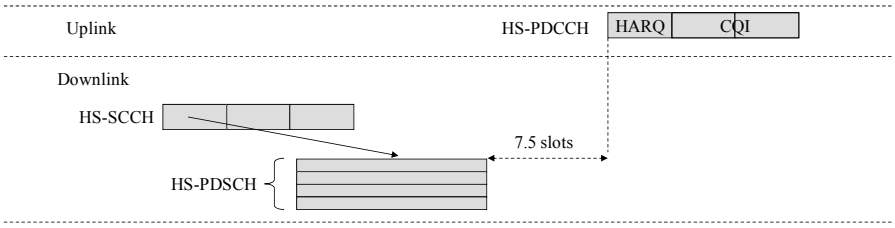


Figure 3.39. *Transmission of the HS-PDCCH*

3.5.2. *HSUPA evolution*

HSUPA (High Speed Uplink Packet Access) evolution is used to increase the rate in the uplink by aggregating the channels. The number and radio characteristics of mobiles are a function of SIR at Node B receiver level that carries out polling to allocate a resource to the mobile. The following functions are available (Table 3.8):

– the allocation of a resource is carried out for a TTI frame of 2 ms or 10 ms, with fast signaling at the level of the physical layer;

– fast scheduling at Node B level;

– retransmission in the event of error or loss is carried out at the level of the physical layer;

– the use of several codes with a SF equal to 2 or 4.

Functions	UMTS	HSDPA
Variable spreading factor	Yes, the value is between 4 and 512 for the downlink 4 and 256 for the uplink	Yes, the value can be equal to 2
Fast power control	Yes	Yes
Adaptive modulation and coding	No	No
Multi-code operation	Yes, rarely used	Yes, 2 SF2 codes and 2 SF4 codes can be used
Retransmission at physical layer level	No, retransmission is ensured by the RLC layer	Yes, retransmission is also ensured by the RLC layer if it fails at physical layer level
Node B scheduling	No	Yes
Soft handover	No	No
Duration of the frame in ms	80, 40, 20, 10	10.2

Table 3.8. *UMTS and HSUPA functions*

3.5.2.1. *MAC layer*

The E-DCH (Enhanced Dedicated CHannel) is obtained from MAC UMTS frames that are encapsulated by a new MAC header, consisting of two entities:

– the MAC-e header dealt with at Node B level;

– the MAC-es header dealt with at RNC level.

The MAC-es header contains the TSN field, identical to that of the MAC-hs header, allowing for the delivery of data in sequence to the RLC layer.

The MAC-e header contains the following fields (Figure 3.40):

– DDI (Data Description Indicator): this field identifies the logical channel and the size of the MAC UMTS frames concatenated in a MAC-es frame.

– N: this field provides the number of consecutive UMTS frames corresponding to the same DDI.

– SI (Scheduling Information): this field contains information on the occupation of mobile queues and the maximum transmission power authorized. This information is used for Node B scheduling data.

Scheduling of E-DCH data from different mobiles is ensured by Node B. The mobile must therefore notify Node B of the state of its queues for transmission.

The processing TrCH (Transport Channel) is applied to a single E-DCH during a TTI that differs from the DCH, where the coded composite transport channel function allows for the simultaneous processing of several transport channels.

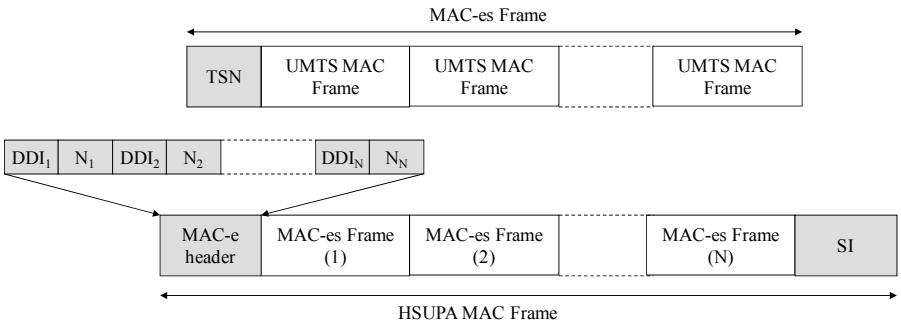


Figure 3.40. *The structure of the MAC-e and MAC-es headers*

3.5.2.2. *The physical layer*

The E-DPDCH (E-DCH Dedicated Physical Data CHannel) is used to support the E-DCH. It allows for the simultaneous transmission of four channelization codes: two codes with a SFof 2 and two codes with a SF of 4, in order to obtain a rate of 5.76 Mbps.

The most notable difference with the DPDCH physical layer concerns the new frame duration of 2 ms that is handled by the physical E-DPDCH. This result is obtained by keeping the structure of the 10 ms frame, but when a TTI of 2 ms is being used the 10 ms radio frame is divided into five independent frames of 2 ms.

The E-DPCCH (E-DCH Dedicated Physical Control CHannel) is used in the uplink to transport control data associated with the E-DPDCH (Figure 3.41). It contains the following information:

– E-TFCI: this field indicates the format of transport transmitted simultaneously on the E-DPDCH;

– RSN (Retransmission Sequence Number): this field indicates the SN of the transport block when sending on the E-DPDCH;

– Happy bit: this indicates whether the mobile is satisfied with the authorized power or whether it could use a more powerful allocation.

The E-HICH (E-DCH HARQ Indicator CHannel) is used in the downlink to transport control data concerning the positive or negative acknowledgement of data received on the E-DPDCH (Figure 3.41).

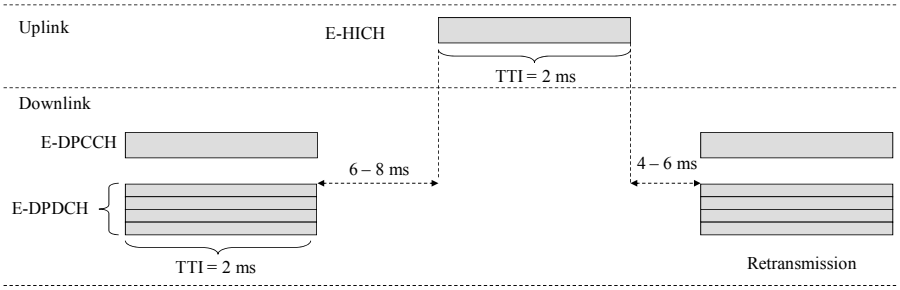


Figure 3.41. *Transmission using the E-DPDCH, E-DPCCH and E-HICH*

The E-DPDCH can also contain a request to obtain a resource allocation. The E-DCH absolute grant channel is used in the downlink to transport control data providing the mobile with the uplink authorization of the user by notifying it of the maximum authorized power, and thus the rate (Figure 3.41).

The E-DCH relative grant is used in the downlink to transport control data notifying the mobile of the relative increase or reduction in the allocated transmission power (Figure 3.41).

3.5.3. *The HSPA+ evolution*

The HSPA+ evolution preserves the HSDPA mode for the downlink and HSUPA for the uplink. The following functions are available to increase the rate in both transmission directions (Table 3.9):

– the use of the MIMO (Multiple Input Multiple Output) system based on the principal of transmitting and receiving two signals on two antennas, using the same radio channel in the downlink;

– the use of 16-QAM modulation in the downstream and 64-QAM in the uplink.

Downlink			
	Modulation	**Propagation**	**Peak rate**
HSDPA	16-QAM	SISO	14.4 Mbps
HSPA+	64-QAM(1)	MIMO (2×2)(2)	43.2 Mbps
Uplink			
	Modulation	**Propagation**	**Maximum rate**
HSUPA	QPSK	SISO	5.76 Mbps
HSPA+	16-QAM(3)	SISO	11.52 Mbps

(1) The modulation gain is equal to 1.5.

(2) The propagation gain is equal to 2.

(3) The modulation gain is equal to 2.

SISO (Single Input Single Output): propagation is carried out via a transmitting antenna and a receiving antenna.

Table 3.9. *The rates in HSPA mode*

In the HSDPA, the mobile must continuously monitor the HS-SCCH. In the HSPA+, the network can limit the number of HS-SCCH frames that the mobile must monitor in order to reduce battery consumption.

The control channel on the HS-DPCCH uplink is important for maintaining the synchronization between Node B and the mobile (for example the level of mobile transmission power). It does, however, contribute to the increase in interference noise at Node B receiver level. Different transmission cycles of this channel are defined in order to reduce the impact on the signal-to-noise ratio.

3.5.3.1. *The MAC layer*

3.5.3.1.1. Downlink

A new MAC-ehs header is introduced to replace the MAC-hs header. It is used to multiplex several logical channels, consider frames of variable lengths and to carry out the segmentation and reassembly of these frames. The MAC-ehs header contains the following fields (Figure 3.43):

– LCH-ID (Logical Channel Identifier): this field is used for identification of the MAC frame or segment and the reorganization queue;

– L (Length): this field provides the size of segment's the MACframe;

– TSN (Transmission Sequence Number): this field provides a SN that is used for the reorganization of data during retransmission;

– SI (Segmentation Indication): this field indicates whether the encapsulated data correspond to a MAC frame or to a segment;

– F (Flag): this field is a flag indicating whether the following field is a LCH-ID field.

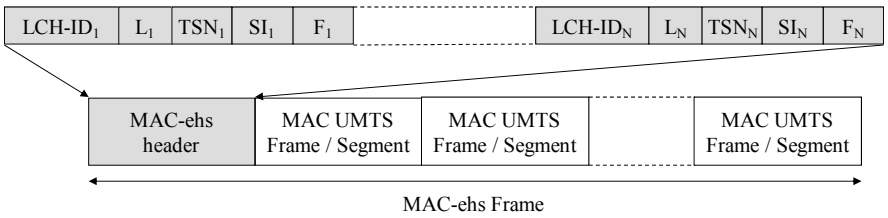


Figure 3.42. *The structure of the MAC-eh header*

3.5.3.1.2. Uplink

Two new MAC-is/i headers are introduced to replace the MAC-es/e headers. As for the downlink, the header is used to consider frames of variable lengths and to carry out the segmentation and reassembly of these frames.

The MAC-is frame can vary in size. The SS (Segmentation Status) and TSN fields of the MAC-is header are repeated for each MAC UMTS frame. The SS field provides an indication on the UMTS frame (Figure 3.44).

The LCD-ID, L and F fields of the MAC-I header are repeated for each MAC UMTS frame to create the MAC-I header of the MAC-is frame. The MAC-i header consists of all MAC-i headers of each MAC-is frame (Figure 3.44).

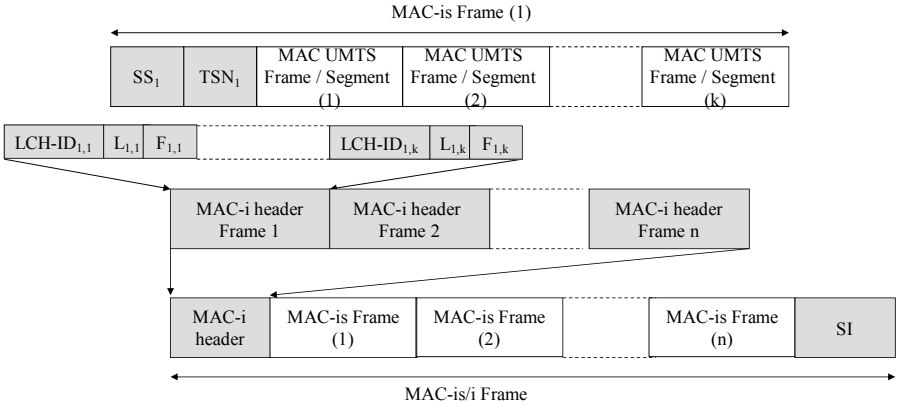


Figure 3.43. *The structure of the MAC-is and MAC-I headers*

3.5.3.2. *Physical layer*

Two independent transport blocks can be transmitted simultaneously on the radio channel, by using the same spreading code. Each transport block is dealt with separately. After the spreading phase, a precoding based on weighting factors (w_1 to w_4) is applied (Figure 3.42).

The first transport block is multiplied by w_1 and w_2, the second by w_3 and w_4. Weight may have the following values:

$$w_1 = w_3 = 1/\sqrt{2}$$

$$w_2 = \left[\frac{1+j}{2}, \frac{1-j}{2}, \frac{-1+j}{2}, \frac{-1-j}{2}\right]$$

$$w_4 = -w_2$$

Node B selects the weighting factor w_2 from the proposition communicated by the mobile on the uplink. The precoding control indication information is signaled by the HS-DPCCH in addition to the CQI.

After multiplication by the weighting factors, the different data flows are added together to create two sources (S_1 and S_2) before their transmission on each antenna.

The mobile must know the weight of w_2 applied to the transmission. The HS-SCCH indicates the value adopted for factor w_2, out of the possible four.

The MIMO system functions on the condition that there are several paths between the sources, S, and the receivers, R. The received signals (R_1 and R_2) are in the form (Figure 3.42):

− $R_1 = h_{11} \times S_1 + h_{12} \times S_2$;

− $R_2 = h_{21} \times S_1 + h_{22} \times S_2$;

− h_{xy} models the propagation between the source, S_x, and the receiver, R_y.

The mobile receiver must therefore be capable of estimating the response, h_{xy}, of the radio channel, and of each transmission antenna. The transmission antennas are therefore required to transmit a different pilot signal:

− one of the antennas transmits the primary (P)-CPICH$_1$ pilot;

− the other antenna transmits either the P-CPICH$_2$ pilot, or the secondary (S)-CPICH$_1$ pilot.

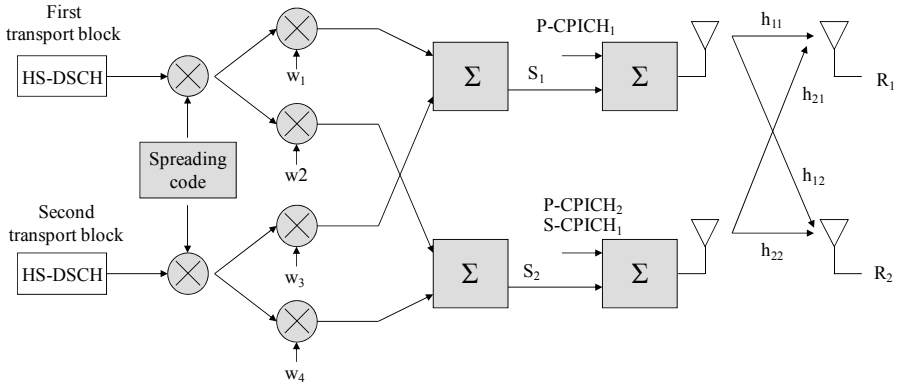


Figure 3.44. *The physical layer*

Chapter 4

The NGN

The basic functions of the MSC (Mobile-services Switching Center), which provides a service in CS (Circuit Service) mode, are circuit switching, signaling processing and mobility management (MM). Interconnection between the entities of the Network Sub-System is achieved by a SDH (Synchronous Digital Hierarchy) transmission network.

The NGN (Next Generation Network) is an evolution of the NNS core network. Signaling processing and MM are provided by a stand-alone entity, the MSC Server. The interconnection between the entities of the NGN is operated by the same Internet Protocol (IP) network deployed for the GSS (GPRS Sub-System).

Section 4.1 explains the architecture of the NGN and describes the components, the MSC Server and the MGW (Multimedia GateWay) and SGW (Signaling GateWay) providing the interfaces with the PLMN (Public Land Mobile Network) or PSTN (Public Switched Telephone Network) third-party networks, BSS (Base Station Sub-system) or UTRANs (UMTS Terrestrial Radio Access Networks).

Section 4.1 also introduces the protocol architecture implemented for signaling and media transport on an IP network, for the control of the gateways by the MSC server and for dialog between the MSC Servers.

Section 4.2 describes the procedures concerning the establishment of a communication during an incoming or outgoing call, release of the communication and management of the mobile on the move (handover).

4.1. Network architecture

4.1.1. *Network components*

The MSC and GMSC (Gateway MSC) nodes are broken down into two entities: the MSC or GMSC Server; and the MGW and SGW (Figure 4.1).

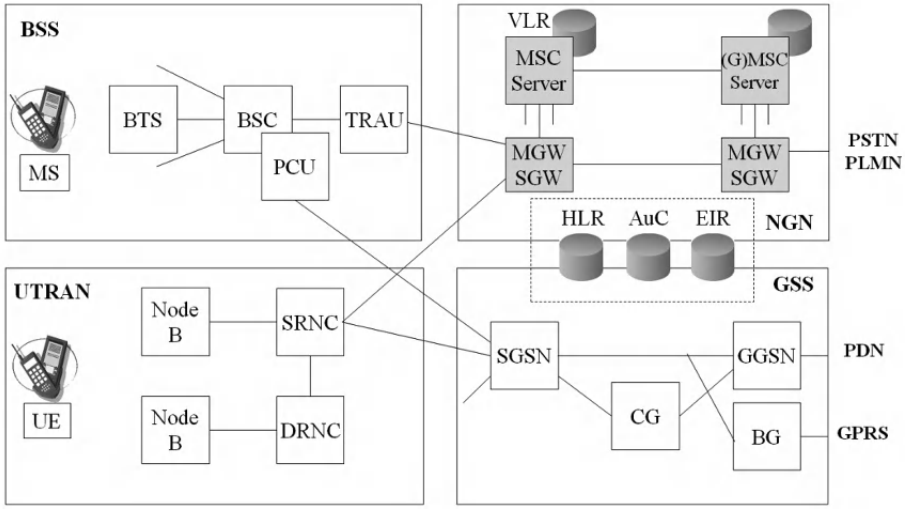


Figure 4.1. *The NGN architecture*

The MSC Server ensures the processing of MM and communication management functions. Like the MSC, it is connected to the Visitor Location Register database to take into account the mobile data stored in the HLR (Home Location Register) database.

The MSC Server terminates the signaling exchanged with the following entities:

– the mobile for CM (Call Management) or MM signaling;

– the BSS access networks for BSSAP (BSS Application Part) signaling or UTRAN for RANAP (Radio Access Network Application Part);

– the PSTN or PLMN third-party networks for ISUP (ISDN User Part) signaling.

BSSAP signaling transports the CM and MM signaling that is exchanged between the MSC Server and the mobile, and the BSSMAP (BSS Management Application Part) signaling, which is exchanged between the BSC and the MSC Server.

RANAP signaling transports CM and MM signaling exchanged between the MSC Server and the mobile. It contains the messages exchanged between the RNC and the MSC Server.

The MSC Server can control several MGW/SGWs, but it is never on a media path. It only carries out signaling processing.

The GMSC Server ensures the particular function corresponding to processing for incoming telephone calls.

The MSC Server ensures the establishment, maintenance and release of connections in the MGW. A connection is a link between an incoming termination (for example the third-party or access network interface) and an outgoing termination (for example the IP network interface) and vice versa.

The MGW carries out protocol conversion relating to multimedia flows between the two terminations. It contains the processing carried out on the media flows, such as transcoding (modification of the type of codec between both terminations), echo cancellation, tone and notification transmission.

The SGW carries out transport protocol conversion relating to signaling exchanged between the MSC Server, and the access networks and third-party networks.

4.1.2. *Protocol architecture*

Different interfaces are defined between the entities that make up the NGN (Figure 4.2):

– the Mc interface between the MGW and the MSC Server supports control of the MGWs by the MSC Server;

– the Nc interface between the MSC Servers supports the signaling exchanged between the MSC Servers, concerning processing of the call;

– the Nb interface between the MGWs supports the transport of media (voice, video and data) on the IP network.

The interface between the SGW and the MSC Server that transports the signaling exchanged between the MSC Server and the access networks or third-party network is unnamed.

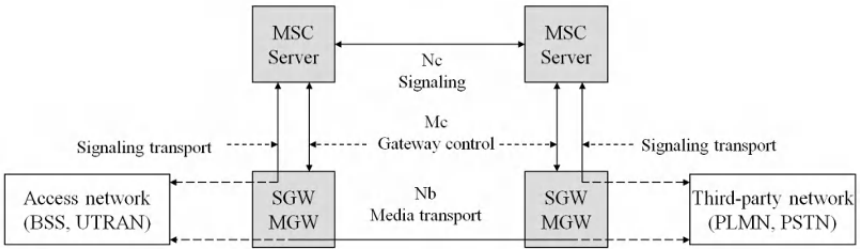


Figure 4.2. *The protocol architecture of the NGN*

4.1.2.1. *Signaling transport*

The SS7 (Signaling System 7) model is applied to BSS access network interfaces, as well as to third-party network interfaces. The SIGTRAN (SIGnaling TRansport over IP) model is used on the NGNs internal interfaces, between the SGW and the MSC Servers. Conversion between the SS7 model and the SIGTRAN model is carried out by the SGW (Figure 4.3).

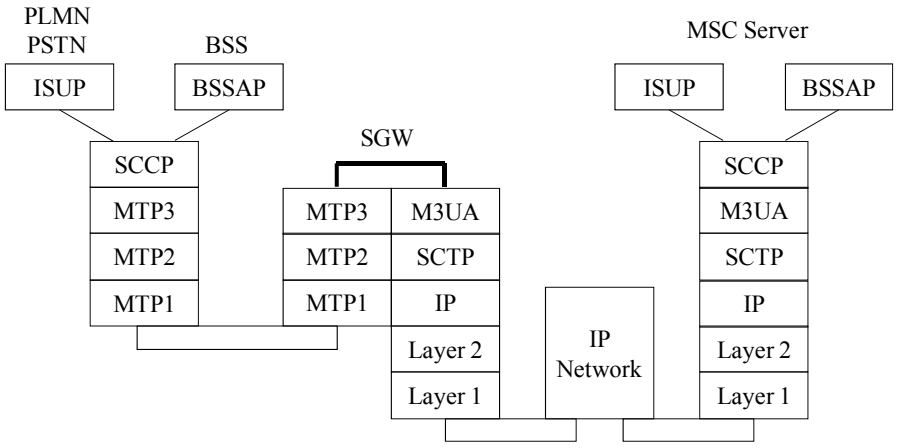


Figure 4.3. *Signaling transport*

The SIGTRAN model defines two SS7 transport protocol layers on the IP:

– the SCTP (Stream Control Transmission Protocol);

– the M3UA (MTP 3 User Adaptation) protocol to signaling protocols exchanged with the access or third-party networks. The M3UA protocol can also be used for the transport of MAP (Mobile Application Part) signaling exchanged with

the databases (HLR, AuC (Authentication Center) and EIR [Equipment Identity Register]) or CAP (CAMEL Application Part) signaling used by the intelligent network entities.

At the UTRAN interface, the structure of SS7 data is adapted for use of the ATM (Asynchronous Transfer Mode) protocol.

The SCTP contains TCP (Transmission Control Protocol) characteristics and offers the following functions:

– a connection to be initialized by the client. During the initialization phase, a cookie is set up to protect against attacks;

– like the TCP, the data are delivered to the application without error and in sequence. If the transfer carried out by the TCP is byte-oriented, that implemented by the SCTP is block-oriented;

– like the TCP, the source rate is regulated by the receiver or the control mechanism for Slow-Start congestion and Congestion Avoidance;

– fragmentation is ensured by the transmitter in order to adapt to the smallest size encountered in the network;

– the messages from several applications can be multiplexed in the same SCTP session;

– several interfaces per host can take part in the connection (multi-homing).

The M3UA protocol is in charge of the primitives between the MTP3 protocol and the protocols of the SCCP (Signaling Connection Control Part) or ISUP top layer, in order to hide the fact that the MTP3 protocol is terminated at SGW level from the MSC Server. The service primitives of the MTP3 protocol are as follows:

– the transfer indication and request, used to exchange data with the top layer;

– the pause indication, used to indicate that the point code is not allocated;

– the resume indication, used to indicate that the point code is available;

– the status indication, used to indicate user availability or congestion.

4.1.2.2. *Voice transport*

The MGW carries out a conversion of the structure of multimedia data (voice, video and data) between the IP network and the access or third-party networks (Figure 4.4).

At the BBS access network or third-party network interface, the TDM (Time Division Multiplexing) structure directly multiplexes the data derived from the G.711 codec in a G.704 frame.

At the UTRAN interface, the data derived from the AMR (Adaptive Multi-Rate) codec is encapsulated by the AAL2 (ATM Adaptation Layer), ATM and SDH protocols.

At the third-party network interface, the MGW also converts the AMR codec format used in the UMTS mobile networks into a G.711 codec, which is normalized for interconnection with the PLMN and PSTN.

At the IP network interface, the channel is encapsulated by the RTP (Real-time Transport Protocol), UDP (User Datagram Protocol) and IP.

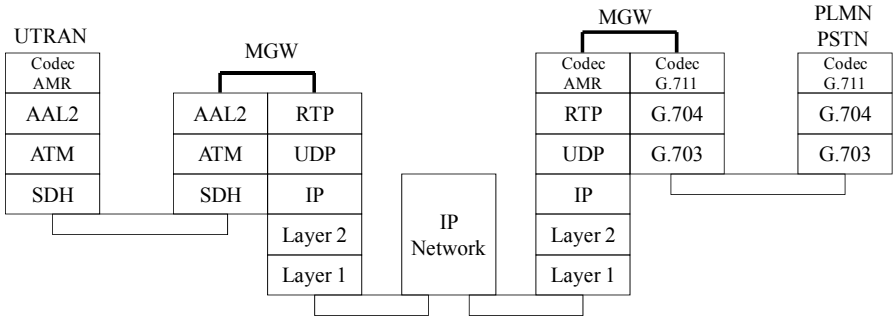


Figure 4.4. *Voice transport*

The UDP cannot be used to detect and correct packet loss in the IP network. This choice is dictated by the impossibility of adopting the TCP, which regulates the source flow, to induce an automatic reduction in rate when there is congestion in the network.

The RTP is the protocol used by real-time applications (voice and video). It is complementary to the UDP to which it is allocated. It provides the following functions:

– identification of codec type;

– the numbering of RTP segments;

– time-stamping of RTP segments.

The RTP contribution to the improvement of vocal quality is due to:

– RTP segment numbering, which can detect lost segments. Each codec has a mechanism that hides this loss from the user;

– RTP segment time-stamping, which can correct the jitter produced by the IP network.

4.1.2.3. *Gateway control*

The MSC Server uses the H.248 or MeGaCo (Media Gateway Controller) protocol to control several MGWs. The connection model describes the logical entities contained in the MGW that the MSC Server can control. The main abstractions used in this connection model are contexts and terminations.

A termination sends and/or collects one or several flows. The media flow parameters are encapsulated in the termination. A context is a package of allocated terminations. The NULL context contains all of terminations that are not allocated to another termination, as is the case with idle time-slots on the interface between the BSC (Base Station Controller) and the MGW.

The H.248 messages have a header that contains the identity of the transmitter and the version of the protocol. Several transactions can be concatenated in a H.248 message. The transactions contained in a message are dealt with independently and no order is predetermined. Each transaction is indicated by a transaction identifier (Figure 4.5).

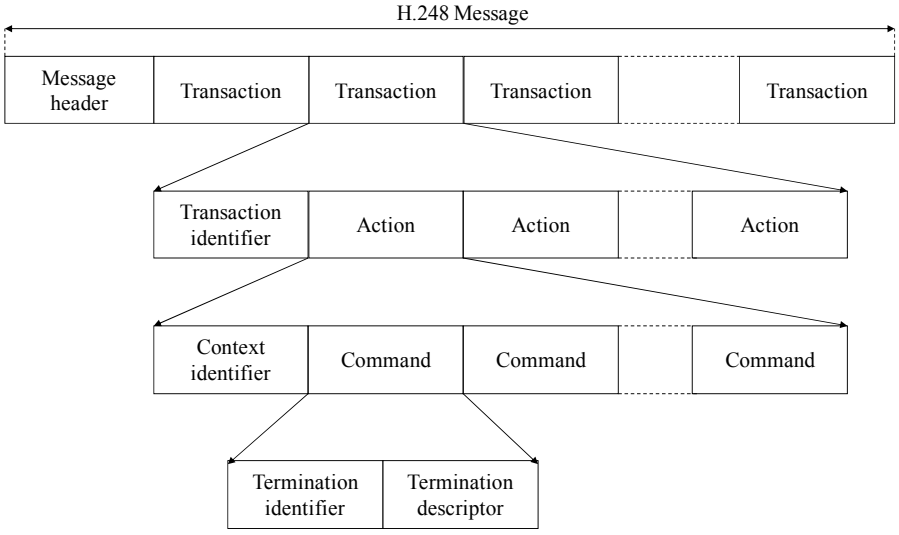


Figure 4.5. *The structure of the H.248 message*

The transactions consist of one or more actions. An action consists of a series of commands to modify or examine the context property. An action usually specifies a context identifier. There is, however, a circumstance when the specific context identifier is not allocated to an action. This is in the creation of a new context requested by the MSC Server.

The descriptor contains the parameters of a termination concerning a command. A descriptor consists of a name and a list of elements. The terminations that are physical entities have a semi-permanent existence, like a time-slot in time-division multiplexing (for the BSC interface). The temporary terminations are RTP (for the IP network interface) or AAL2 (for the RNC interface) flows.

The protocol provides commands to manipulate the logical entities of the connection model, the contexts and the terminations:

– ADD: this command adds a termination to a context. Applied to the first termination of a context, it also serves to create a context;

– MODIFY: this command modifies the properties of a termination;

– SUBTRACT: this command disconnects a termination from its context and sends back statistics about the participation of this termination in this context. Applied to the last termination of a context, it serves to cancel the context;

– MOVE: this command moves a termination to another context;

– AuditValue: this command sends back the current states of the properties and statistics associated with the terminations;

– AuditCapabilities: this command sends back all the possible values of termination properties authorized by the MGW;

– NOTIFY: this command allows the MGW to inform the MSC Server about the development of events in this gateway;

– ServiceChange: this command allows the MGW to signal to the MSC Server that a termination or a group of terminations is about to be disabled or has just be enabled. This command is also used by the MGW to register with the MSC Server. The MSC Server can also use this command to request that the MGW enable or disable a termination or group of terminations.

Most commands are reserved for the specific use of the MSC Server to control the MGWs. The exceptions are the NOTIFY and ServiceChange commands, the first being sent by a MGW and the second being able to be sent by one of the two entities.

4.1.2.4. *Signaling between the MSC Servers*

The BICC (Bearer Independent Call Control) protocol is used for the signaling exchanged between the MSC Servers. It was developed from the ISUP protocol, which is fundamentally similar with regards to basic call procedures and the additional functions of telephone services.

The BICC protocol also implements a mechanism that allows for the exchange of information linked to the media flow bearer command on the IP network between the MGWs. This information concerns the IP addresses, the UDP port numbers, the types of media (voice, video and data) and the formats used for this media (codecs for voice and video; protocols for data).

This information is tunnelized in BICC messages containing signaling, such as the IAM (Initial Address Message) for communication establishment or in the BICC APM (APplication transport Mechanism) message, which does not transport any signaling information (Figure 4.6).

The IPBCP (IP Bearer Control Protocol) is a media flow bearer control protocol that aims to ensure the exchange of necessary information in order to establish or modify media flow characteristics (Figure 4.6). It is initialized by the MGW and is passed to the MSC Server thanks to the H.248 protocol, for which a specific package is defined. The package defines additional properties that can appear in the terminations and contexts.

The IPBCP defines four types of message:

– the request message (REQUEST) is sent by a MSC Server entity in order to launch a request to establish or modify a media flow on the IP network;

– the acceptance message (ACCEPTED) is sent by the MSC server entity that receives a message of media flow establishment or modification, if it accepts the request;

– the error message (CONFUSED) is sent by the MSC Server entity in response to a media flow modification or establishment if it cannot deal with the received request message;

– the refusal message (REJECTED) is sent by the MSC Server entity in response to a request for media flow establishment or modification if it refuses the request.

The BCTP (Bearer Control Tunneling Protocol) is used for the tunnelization of media flow bearer control protocols on the BICC protocol (Figure 4.6). The header of the BCTP contains the following indications:

– BCTP version error;

– the version of the BCTP;

– a version error of the control protocol of the media flow bearer;

– the type of media flow bearer control protocol.

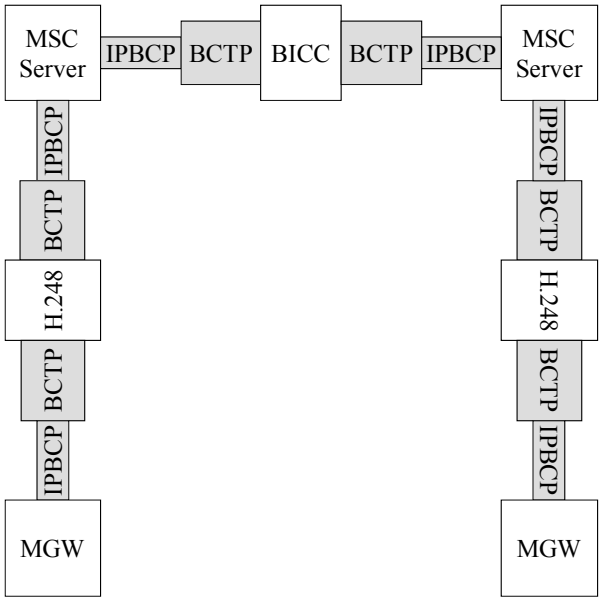


Figure 4.6. *Tunnelization of the IPBCP message*

4.2. Communication management

4.2.1. *Communication establishment*

4.2.1.1. *The outgoing call*

The outgoing call is generated by the mobile by sending the CM SET UP message. The MSC Server responds to this with the CM CALL PROCEEDING message. Upon receiving the SET UP message, the local MSC Server selects the MGW in order to establish media flow on the IP network. An H.248 (ADD message) transaction is transmitted to the local MGW to create a context and a T2 termination (for the IP network). The local MGW responds with the identifiers for the new context and the termination that has been created. The media flow options are sent in an IPBCP request (Figure 4.7).

The local MSC Server creates the BICC IAM and transmits it to the remote MSC Server. This message also supports the IPBCP request describing the media flow options of the MGW (Figure 4.7).

The remote MSC Server will create a context and a termination from the IP network on its own MGW by using the ADD message. This message also contains the IPBCP message received from the local MSC. The remote MGW responds with the characteristics of the termination created from the IP network in the IPBCP message. This response is encapsulated in a BICC APM and is then sent back to the local MSC Server (Figure 4.7).

The local MSC Server transmits the IPBCP response to the local MGW by using the MODIFY command. At this stage, the media flow bearer on the IP network is defined at each termination (Figure 4.7).

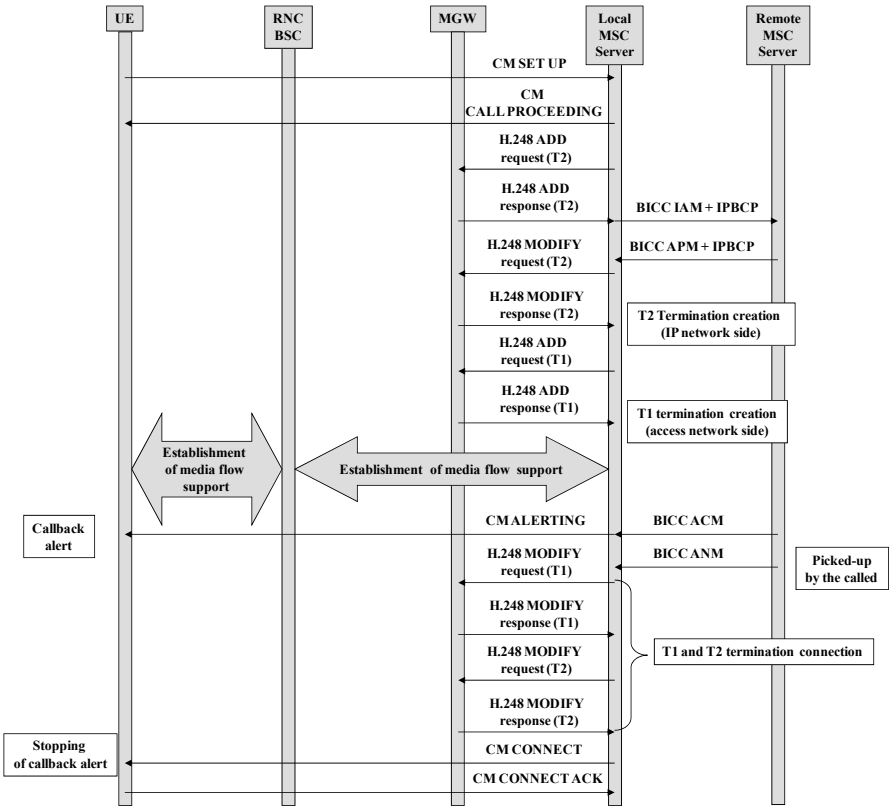


Figure 4.7. *The establishment phases of an outgoing call*

The second stage consists of preparing the media flow bearer from the access network. For this, the MSC Server uses the ADD command to create the T1 termination on the BSC or RNC interface. Upon response from the MGW, the MSC Server proceeds to establish the bearer by using BSSAP signaling with the BSC or RANAP with the RNC (Figure 4.7).

Upon receiving the BICC ACM from the remote MSC Server, the local MSC Server sends the CM ALERTING message to the person calling, which triggers the callback alert (Figure 4.7).

When the person requested picks up, the local MSC Server receives the BICC ANM. It orders the connection between both terminations T1 and T2 of the MGW thanks to the MODIFY command. The CM CONNECT message is sent to the person calling in order to interrupt the alert. The mobile acknowledges the received CM CONNECT message by responding with the CM CONNECT ACK message (Figure 4.7).

4.2.1.2. *The incoming call*

The procedures concerning the incoming call follow the chronology described in the GSM network. Upon receiving an ISUP IAM, the GMSC Server contacts the HLR to get the identity of the MSC Server on which the mobile is recorded. It creates two T3 (from the third-party network) and T4 (from the IP network) terminations on its MGW. It then transmits the BICC IAM to the MSC Server with the IPBCP message containing the characteristics of the termination created on the IP network (Figure 4.8).

Upon receiving the BICC IAM, the MSC Server creates two T1 (for the access network) and T2 (for the IP network) terminations at MGW level. It sends back the APM to the GMSC Server with the IPBCP message containing the characteristics of the termination created on the IP network. The GMSC relays this message to its MGW in order to modify the T4 termination (Figure 4.8).

The MSC Server initiates the call procedure with the requested mobile and the establishment of the media flow bearer in the access network. When the person requested responds with the CM CONNECT message, the MSC Server establishes the connection between both T1 and T2 terminations created in the MGW. It transmits the BICC ANM to the GMSC Server (Figure 4.8).

Upon receiving this message, the GMSC Server establishes the connection between both T3 and T4 terminations of its MGW (Figure 4.8).

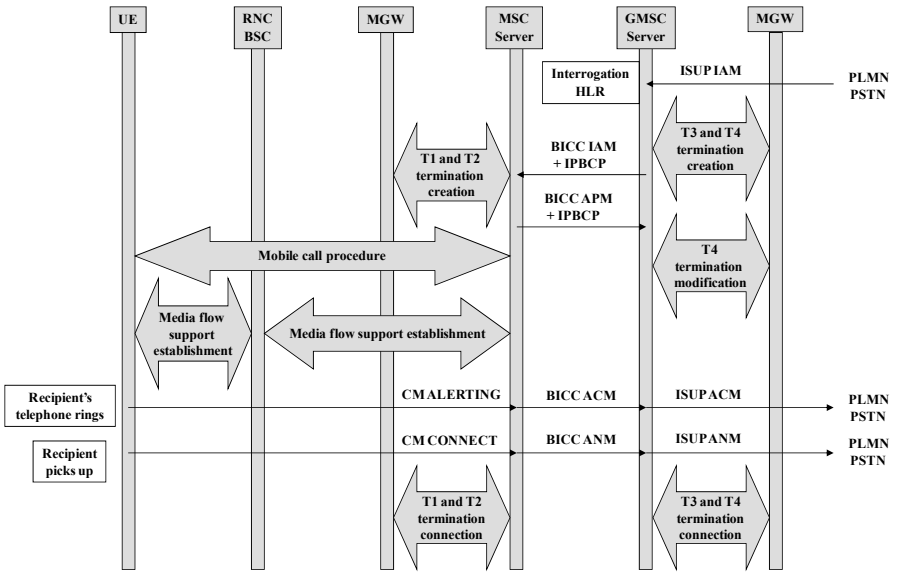


Figure 4.8. *The establishment phases of an incoming call*

4.2.2. *Communication release*

Communication release can be initialized by the users when the person who is being requested or the person requesting hangs up. It can also be initialized by the entities of the NGN (MSC Server, GMSC Server or MGW) or by the access network in the event of radio link loss with the mobile. The following example deals with the instance when the mobile of the person requesting hangs up first (Figure 4.9).

When the person requesting hangs up, the transmission of a CM DISCONNECT message is triggered. Upon receiving this message, the MSC Server carries out the following operations (Figure 4.9):

– it transfers the BICC REL message to the remote MSC Server;

– it responds to the person calling with the CM REL message. The person calling confirms receipt of this message by sending the CM RLC message;

– it provokes the release of the access network resources;

– it proceeds to disconnect T1 and T2 terminations of the MGW (MODIFY command), then withdraws these terminations (SUBTRACT command).

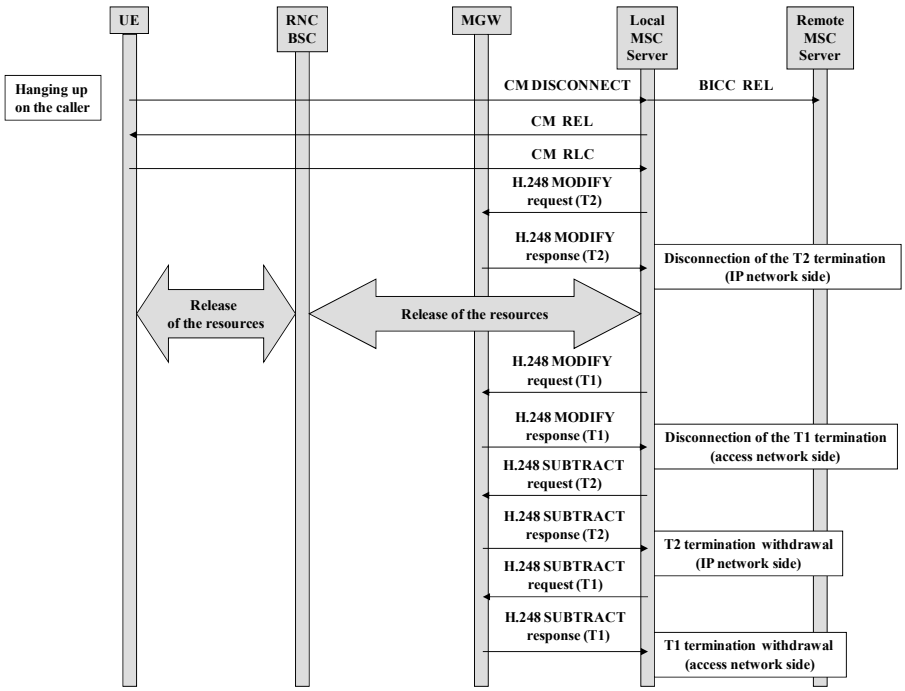


Figure 4.9. *Communication release phases*

4.2.3. *The handover*

4.2.3.1. *The intra-MSC handover*

The intra-MSC handover arises when the mobile changes the cell and the BSC or RNC that is serving it, but always depends on the same MSC Server. The original and destination BSCs or RNCs, however, can be connected to two different MGWs.

The intra-MSC handover can be an intra-system handover (a change from one BSC to the other or from one RNC to another) or inter-system (a change from a BSC to a RNC or *vice versa*). The procedure described as an example concerns the UMTS intra-system handover.

Before initializing the handover procedure, the original RNC is connected to the MGW on the T1 termination. The interface of the MGW on the IP network to the remote gateway uses the T2 termination (Figure 4.10).

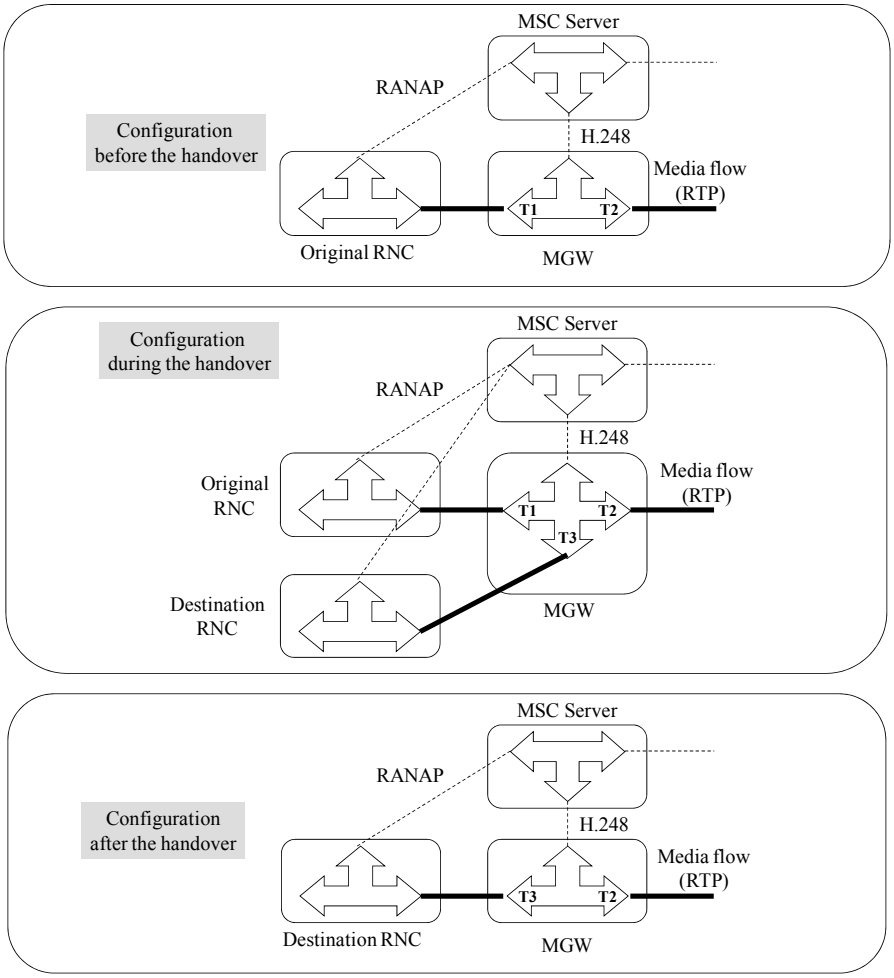


Figure 4.10. *Configuration during handover*

During the handover phases, the MSC Server carries out the following operations on the MGW (Figure 4.10):

– creation of the T3 termination, at the destination RNC interface;

– disconnection of T1 and T2 terminations;

– connection of T2 and T3 terminations;

– cancellation of the T1 termination.

The MSC Server receives the RANAP RELOCATION REQUIRED message from the original RNC. It uses the "Prepare Bearer" procedure (add request from a termination via the H.248 ADD command) in order to create a new T3 termination (on the destination RNC). It uses the "Change Flow Direction" procedure (termination modification request with the H.248 MODIFY command) to disconnect the T1 and T2 terminations. It sends the RANAP RELOCATION REQUEST message to the destination RNC while notifying it of the media flow bearer characteristics (Figure 4.11).

When the MSC Server receives the RANAP RELOCALISATION REQUEST ACK message from the destination RNC, it uses the "Change Flow Direction" procedure to establish a connection between the T2 and T3 terminations (Figure 4.11).

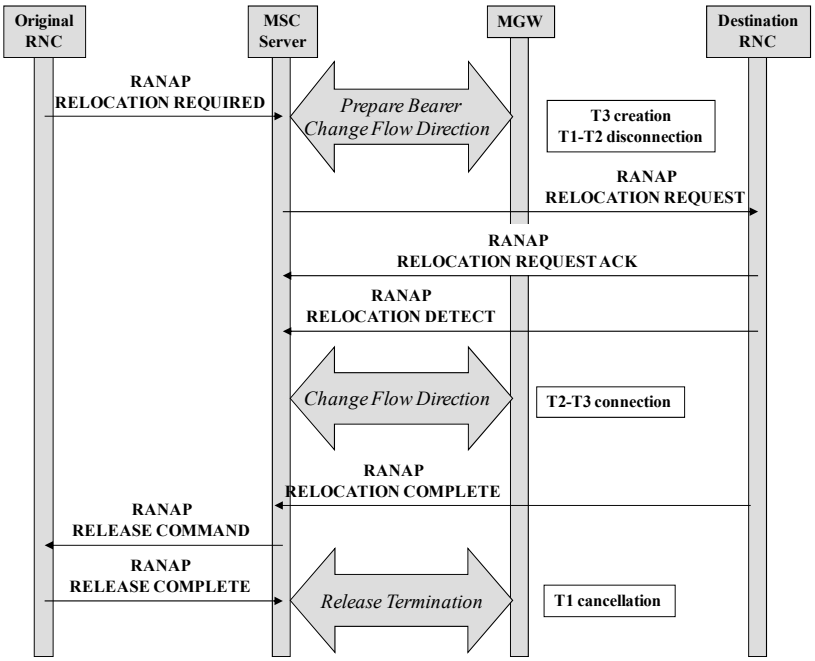


Figure 4.11. *The establishment phases of the UMTS intra-system intra-MSC handover*

Upon receiving the RANAP RELOCATION COMPLETE message, the MSC Server sends the RANAP RELEASE COMMAND message to the original RNC to release the resources on the UTRAN. When the MSC Server receives the RANAP RELEASE COMPLETE message from the original RNC, it uses the "Release Termination" procedure (request for the withdrawal of a termination with the H.248 SUBTRACT command) to cancel the T termination (Figure 4.11).

4.2.3.2. *The inter-MSC handover*

The inter-MSC handover arises when the mobile changes cell, BSC or RNC, MSC Server and MGW. The inter-MSC handover can be an intra- or inter-system handover. The procedure described as an example concerns the UMTS intra-system handover.

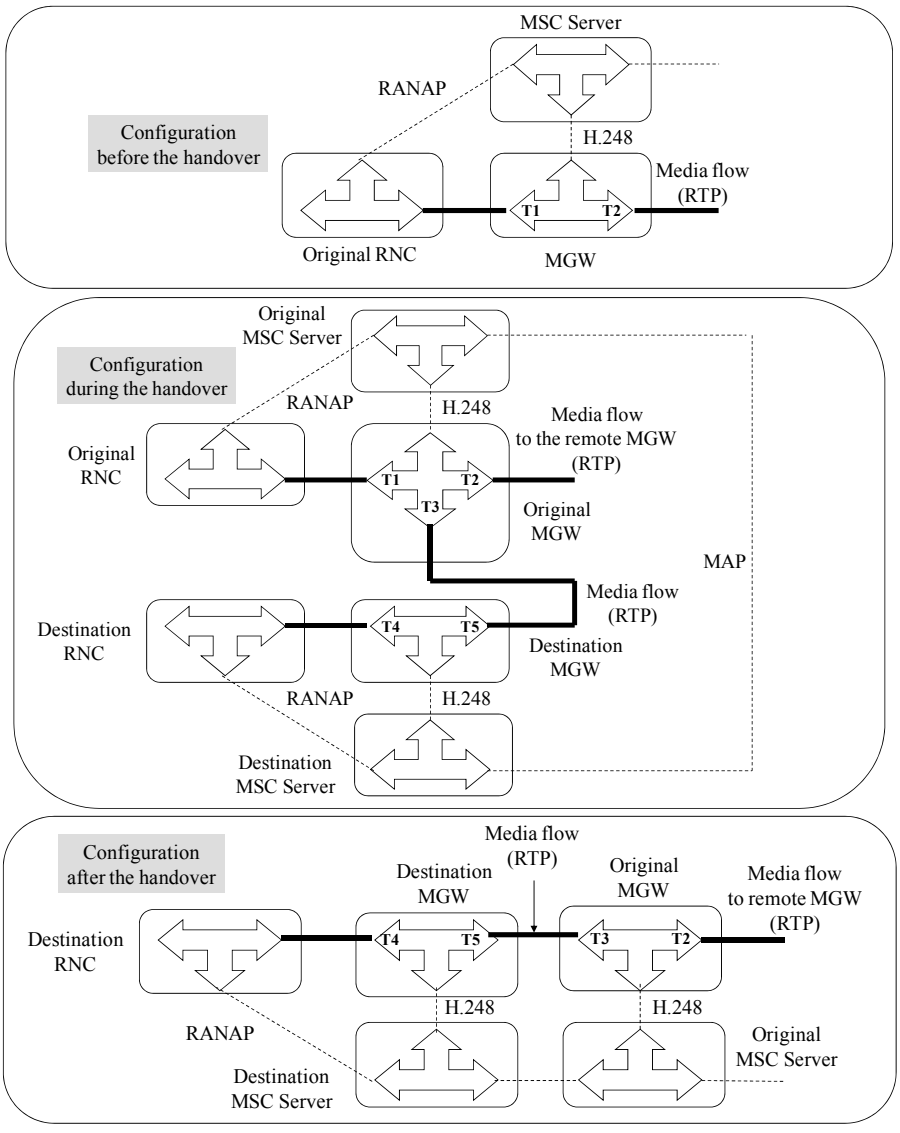


Figure 4.12. *Configuration during the handover*

During the handover phases, the original MSC Server carries out the following operations on the original MGW (Figure 4.12):

– creation of the T3 termination at the IP network interface;

– disconnection of T1 and T2 terminations;

– connection of T2 and T3 terminations;

– suppression of the T1 termination.

During the handover phases, the destination MSC Server carries out the following operations of the destination MGW (Figure 4.12):

– creation of the T5 termination at the IP network interface;

– creation of the T4 termination, at the destination RNC interface;

– connection of T4 and T5 terminations.

Upon receiving the RANAP RELOCATION REQUIRED message from the original RNC, the original MSC Server indicates in a MAP PREPARE HANDOVER REQUEST message to the destination MSC Server, the list of codecs supported by the mobile and the codec used in the current communication (Figure 4.13).

The destination MSC Server uses the "Prepare Bearer" procedure to create a new T5 termination and it dispatches the RANAP RELOCATION REQUEST message to the destination RNC while notifying it of the media flow bearer characteristics (Figure 4.13).

When the destination MSC Server receives the RANAP RELOCALISATION REQUEST ACK message from the destination RNC, it uses the "Prepare Bearer" procedure in order to create the T4 termination with the destination RNC and responds to the original MSC with the MAP PREPARE HANDOVER RESPONSE message (Figure 4.13).

The original MSC Server uses the "Prepare Bearer" procedure in order to create the T3 termination with the IP network and the "Change Flow Direction" procedure to disconnect the T1 and T2 terminations (Figure 4.13).

The implementation of the media flow bearer between the T3 and T5 terminations is accomplished via the exchange of BICC APMs encapsulating the IPBCP media flow bearer command (Figure 4.13).

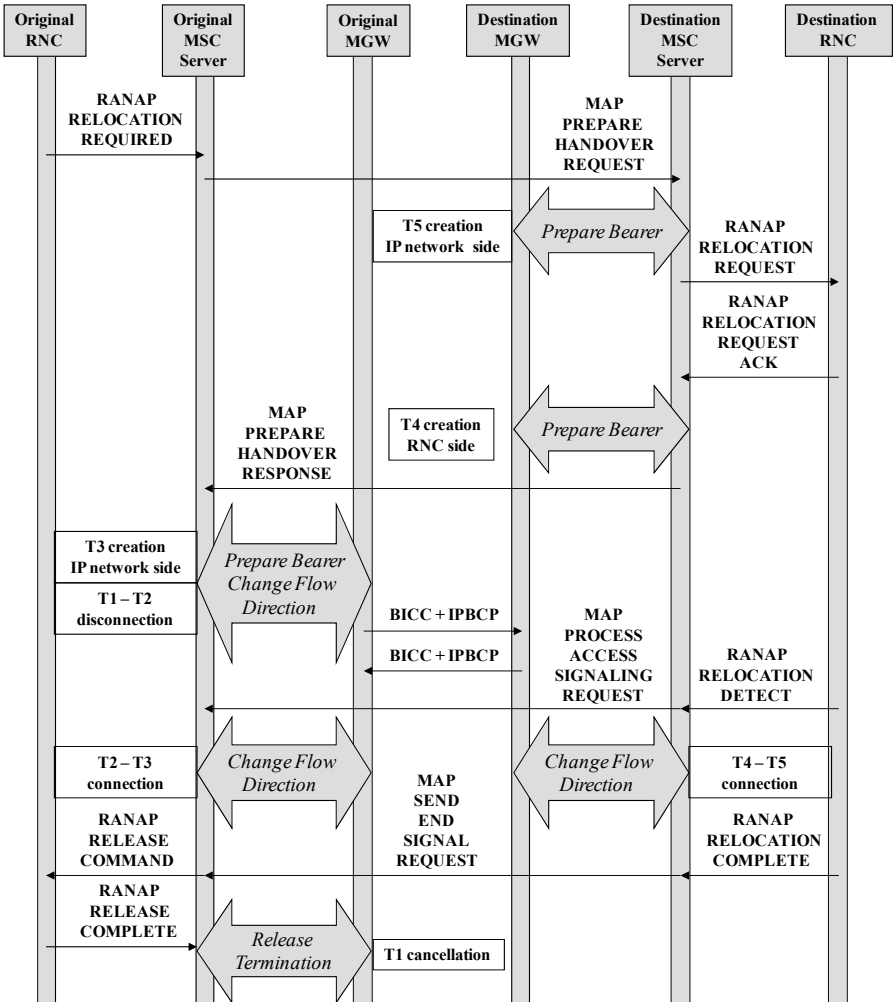


Figure 4.13. *The establishment phases of the UMTS intra-system inter-MSC handover*

Upon receiving the RANAP RELOCATION DETECT message, the destination MSC Server uses the "Change Flow Direction" procedure to connect the T4 and T5 terminations. It then sends the MAP PROCESS ACCESS SIGNALING REQUEST message to the original MSC Server, which sets up the connection between the T2 and T3 terminations (Figure 4.13).

Upon receiving the RANAP RELOCATION COMPLETE message, the destination MSC Server sends the MAP SEND END SIGNAL REQUEST message

to the original MSC Server. The latter releases the UTRAN resources while sending the RANAP RELEASE COMMAND message to the original RNC. When the original MSC Server receives the RANAP RELEASE COMPLETE message from the original RNC, it uses the "Release Termination" procedure to cancel the T1 termination (Figure 4.13).

Chapter 5

The EPS Network

The EPS (Evolved Packet System) network is unusual with regards to the 2G (GSM (Global System for Mobile)/GPRS (General Packet Radio Service)) and 3G (UMTS, Universal Mobile Telecommunications System) networks, it only offers a data transmission service in PS (Packet Service) mode, whose main characteristic is that it increases the peak rate.

In order to provide a telephone service, the EPS network only produces voice and signaling transport, which are considered to be data. Signaling and voice processing is carried out by the IMS (IP Multimedia Subsystem) network, outside of the mobile network.

Section 5.1 explains the architecture of the EPS mobile network, which consists of two sub-systems: the eUTRAN (evolved Universal Terrestrial Radio Access Network); and the EPC (Evolved Packet Core) network and UE (User Equipment) mobiles.

Section 5.2 develops the characteristics of the physical layer of the radio interface. After dealing with the radio resource access mode, the section continues with the detailed description of the signals and the physical channels.

Section 5.3 sets out the procedures concerning the establishment of a connection between the mobile and the connecting radio station, the mobile's location update, session establishment and intra- and inter-system handover management.

5.1. Network architecture

5.1.1. *Network components*

The EPS network consists of an EPC network and an eUTRAN access network. The EPS network only offers a data transmission service in PS mode.

The term SAE (System Architecture Evolution) is assigned to the study of the evolution of the core network. EPC is the term reserved to denote the core network.

The term LTE (Long-Term Evolution) is assigned to the study of the evolution of the radio interface. eUTRAN is the term reserved to denote the access network.

The EPC core network (Figure 5.1) includes:

− the MME (Mobility Management Entity) signaling processing entity;

− the SGW (Serving GateWay) and PGW (PDN [Packet Data Network] GateWay) data transfer entities;

− the HSS (Home Subscriber Server) and EIR (Equipment Identity Register) mobile databases;

− the PCRF (Policy and Charging Rules Function) entity, which defines the quality of service and charging rules.

The EPC core network has the following differences compared with the GSS core network of the 2G and 3G mobile networks:

– a specific MME is responsible for signaling exchange with the mobile and the access network. In the case of the 2G and 3G networks, these functions are achieved by the SGSN (Service GPRS Support Node);

– two anchor points (SGW and PGW) are created. In the 2G and 3G networks, the single anchor point is ensured by the GGSN (Gateway GPRS Support Node).

The MME manages and stores the contexts relating to mobiles:

– the mobile's private IMSI (International Mobile Subscriber Identity);

– the temporary private GUTI (Globally Unique Temporary Identity);

– the location TAI (Tracking Area Identity);

– the authentication and encryption data;

– the mobile's capabilities;

– the quality of service assigned to the bearer.

The MME is responsible for mobility management, attachment and detachment and the TAI location area update. It manages the authentication procedure and the allocation of the GUTI. It transfers the mobile's context to the SGSN during the inter-system (EPS to UMTS) mobility.

The SGW entity also manages and stores the contexts relating to mobiles:

– the mobile's IP address;

– the quality of service assigned to the bearer;

– the IP addresses of the eNode B and PGW entities;

– the identifier of the TEID (Tunnel Endpoint IDentifier) mobile session.

The SGW entity transfers the incoming data to the eNode B entity and the outgoing data to the PGW entity. It initializes paging to the MME for the incoming data. It is the anchor point for the intra-eUTRAN mobility. During the inter-system mobility, it transfers the data to the SGSN or RNC of the UMTS network.

The PGW entity ensures connection of the EPS network to the fixed PDN (the Internet network). It is the equivalent of the GGSN entity of the UMTS network. It is responsible for IP address allocation to the mobile. It is the anchor point for the inter SGW mobility.

The PGW entity hosts the PCEF (Policy and Charging Enforcement Function) that inspects the data received from the fixed SGW or PDN, marks the IP packets for the incoming data according to the quality of service applied to the bearer, and generates the charging tickets intended for the CG (Charging Gateway) entity.

The HSS database is an integration of the functions fulfilled by the HLR (Home Location Register) and AuC (Authentication Center) database.

The PCRF entity provides the PCEF of the PGW entity with the rules that need to be applied for charging and quality of service when the bearer must be established for the mobile[1]. When the mobile is connected to the visitor network, the PCRF entity of the host network is connected to the PCRF entity of the visitor network. When the telephone service is provided by the IMS (IP Multimedia Service) network, the latter provides the rules to be applied.

The eUTRAN is simplified and includes a single type of entity, the eNode B radio station that integrates the functions previously assigned to the BSC station controllers of the 2G and RNC networks of the 3G networks (Figure 5.1).

1 The PCRF can also be connected to the PCEF that is integrated in the GGSN entity of the UMTS network.

The eNode B entity is responsible for radio resource management, control of bearer allocation to the mobile and its mobility. It carries out the compression and encryption of data on the radio interface.

The eNode B entity routes the mobile data to the SGW entity and carries out IP packet marking for the outgoing data according to the quality of service allocated to the bearer.

The eNode B entity carries out selection of the MME allocated to a mobile. It deals with the paging request transmitted by the MME for its transmission in the cell.

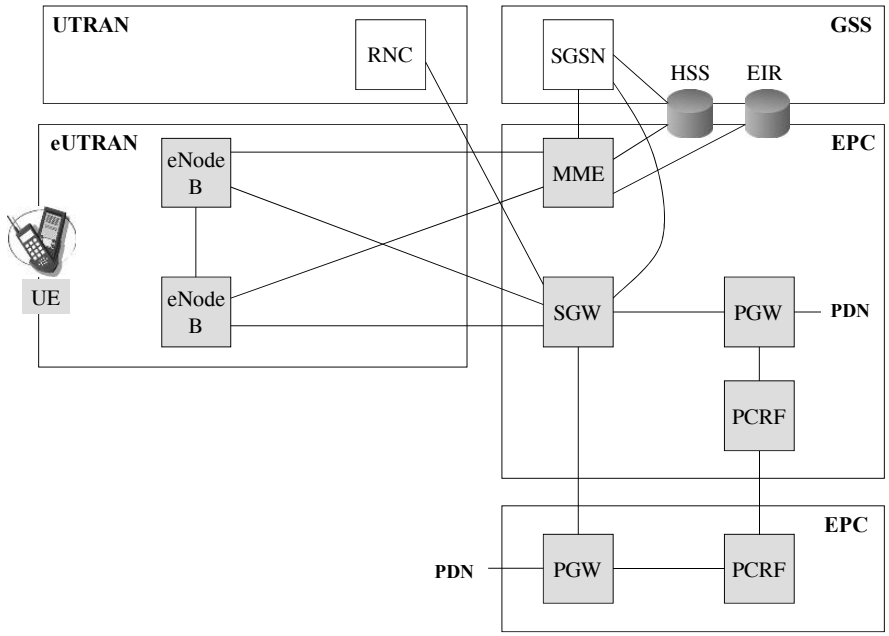


Figure 5.1. *The architecture of the EPS network*

5.1.2. *Protocol architecture*

5.1.2.1. *The reference points*

There are a number of reference points:

− Uu: this is a reference point between the mobile and the eNode B entity for signaling (Figure 5.2) and traffic (Figure 5.3). The mobile's signaling is exchanged with the eNode B entity by the RRC (Radio Resource Control) protocol and with the

MME by the NAS (Non Access Stratum) protocol, which corresponds to mobility and session management.

− S1-MME: this is the reference point between the MME and the eNode B entity for signaling via the S1-AP (Application Part) protocol exchanged during mobile attachment, the establishment of a session and intra-eUTRAN handover based on the S1 interface (Figure 5.2).

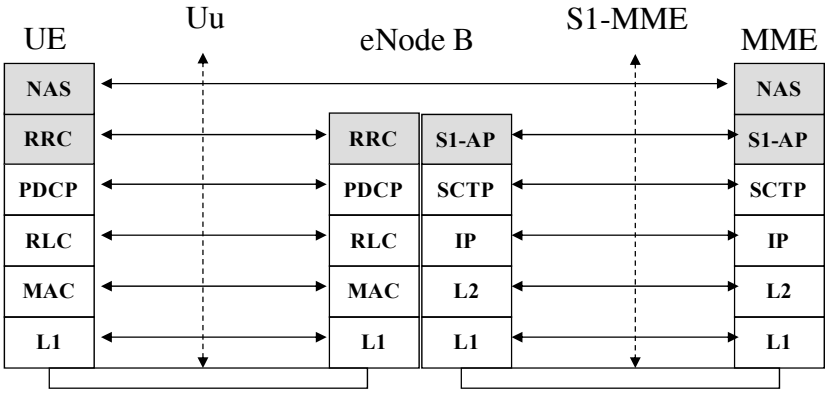


Figure 5.2. *Reference points Uu and S1-MME − the control plane*

− S1-U: this is the reference point between the eNode B and SGW entities for tunneling via the GTP-U (GPRS Tunnel Protocol User) protocol of the mobile traffic (the IP packet), see Figure 5.3.

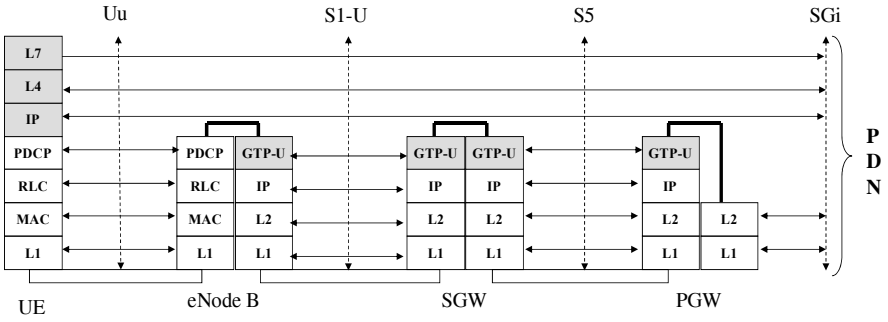


Figure 5.3. *Reference points Uu, S1-U, S5 and SGi − the traffic plane*

− S3: this is the reference point between the MME and SGSN entity for signaling via the GTP-C (GTP-Control) protocol, exchanged during inter-system handover.

− S4: this is the reference point between the SGW and SGSN entities for signaling exchange via the GTP-C protocol and tunneling via the GTP-U mobile traffic protocol during inter-system handover.

− S5: this is the reference point between the SGW and PDW entities for tunneling via the GTP-U mobile traffic protocol (Figure 5.3) and for signaling via the GTP-C protocol concerning the management of the tunnel and handover, with relocation of the SGW entity.

− S6a: this is the interface point between the MME and HSS entity for signaling via the DIAMETER protocol, which provides access to the mobile data (authentication, service profile), see Figure 5.4.

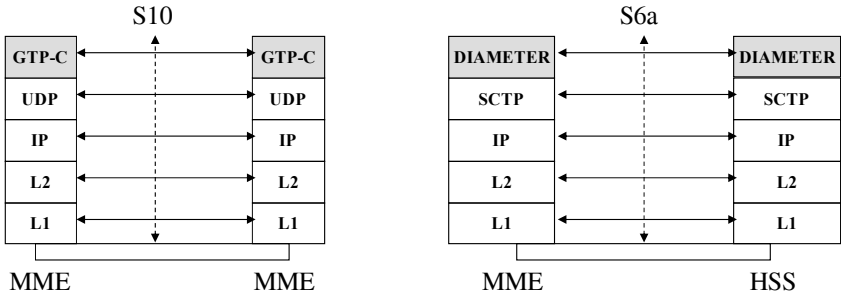


Figure 5.4. *Reference points S6a and S10*

− S8: this is the reference point between the SGW entity of the visitor network and the PDW entity of the host network, variant of the reference point S5.

− S9: this is the reference point between the PCRF entities of the host and visitor networks for signaling (the DIAMETER protocol), which concerns the transfer of quality of service and charging rules.

− S10: this is the reference point between the MMEs for signaling via the GTP-C protocol, exchanged for the relocation of this entity during a relocation handover (Figure 5.4).

− S11: this is the reference point between the MME and SGW entity for signaling via the GTP-C protocol. It is exchanged during mobile attachment, the establishment of a session and during the handover with relocation of the SGW entity.

− S12: this is the reference point between the RNC and SGW entities for direct tunneling via the GTP-U protocol, of the mobile traffic during the inter-system handover.

− S13: this is the reference point between the MME and EIR entity for signaling via the DIAMETER protocol. It concerns control of the mobile's IMEI.

− SGi: this is the reference point between the PDW entity and the fixed PDN (Figure 5.3).

− Gx: this is the reference point between the PCRF and PCEF entities for signaling via the DIAMETER protocol. It concerns the transfer of the rules of quality of service and charging.

− X2: this is the reference point between two eNode B entities for signaling via the X2-AP protocol and tunneling via the GTP-U protocol of the mobile traffic (the IP packet) when it changes cell (Figure 5.5).

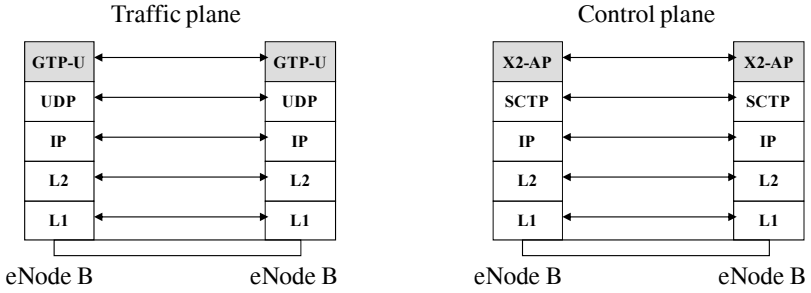


Figure 5.5. *Reference point X2*

5.1.2.2. *The Uu interface*

Three channel levels are defined on the radio interface (Figure 5.6):

– The logical channel defines the type of information. It corresponds to the data structure at the interface between the RLC (Radio Link Control) and MAC (Medium Access Control) layers. The logical channels are classified into two groups: traffic channels and control channels.

– The transport channel defines the format of the data. It corresponds to the structure of data at the interface between the MAC layer and the physical layer. The data are transmitted to the physical layer in the form of blocks. One or two blocks are delivered for each TTI (Transmission Time Interval) time-slot in 1 ms.

– The physical channel defines the resource allocated to the transport channel and its position in the frame. The physical channels are described in section 5.2.

5.1.2.2.1. Logical channels

The BCCH (Broadcast Control CHannel) is a common unidirectional control channel that is used solely in the downlink to broadcast system information. The MIB (Master Information Block) is transmitted in the BCH (Broadcast CHannel). The SIB (System Information Block) is transmitted in the DL-SCH (DownLink Shared CHannel).

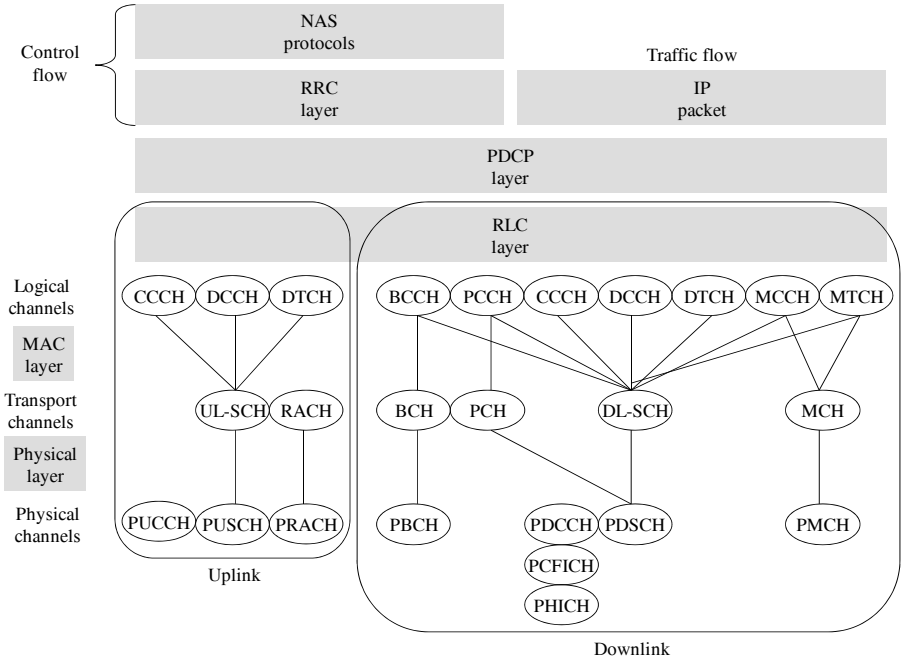


Figure 5.6. *The logical, transport and physical channels*

The MIB contains a minimum of information concerning the bandwidth of the radio channel and the configuration of the PHICH (Physical HARQ Indicator CHannel).

SIB1 gives instructions to the mobile regarding the identity of the mobile network, the code of the TAI location, the identity of the cell, the minimum power to use in the cell and the configuration of the sub-frame in TDD (Time Division Duplex) mode.

SIB2 provides information that allows the mobile to access the cell. It includes the bandwidth of the cell's radio channel, the parameters concerning random access and the power control.

SIB3 contains the information concerning reselection of the cell.

SIB4 to SIB8 provide information concerning the neighboring cells that are functioning on different or identical frequencies and the neighboring cells of the GSM or UMTS networks.

The PCCH (Paging Control CHannel) is a common unidirectional control channel that is used solely in the downlink to transport paging information. This channel is mapped in the transport PCH (Paging CHannel).

The CCCH (Common Control CHannel) is a common bidirectional control channel that is used to transmit the first RRC signaling messages. This channel is mapped in the UL-SCH (UpLink SCH) and DL-SCH.

The DCCH (Dedicated Control CHannel) is a dedicated bidirectional control channel that is used to transmit the RRC messages. This channel is mapped in the UL-SCH and DL-SCH.

The MCCH (Multicast Control CHannel) is a unidirectional channel used in order to transmit control information associated with multicast traffic. This channel is mapped on the transport MCH (Multicast Channel) if the multicast traffic is solely transmitted in the cell, or on the DL-SCH if the multicast traffic is broadcast on several cells.

The DTCH (Dedicated Traffic CHannel) is a dedicated bidirectional channel that transmits unicast traffic data (the IP packet). This channel is mapped in the UL-SCH and DL-SCH.

The MTCH (Multicast Traffic CHannel) is a unidirectional channel that transmits multicast data to the mobile. Like the MCCH, this channel is mapped in the transport MCH or in DL-SCH.

5.1.2.2.2. Transport channels

The BCH supports the system information contained in the MIB. This channel is mapped in the physical PBCH.

The PCH transports the logical PCCH. It supports the discontinuous transmission at predefined times in order to allow the mobile to save its battery. This channel is mapped in the PDSCH (Physical Downlink Shared CHannel).

The DL-SCH is the main channel in the downlink. It can transport all logical channels. In particular, it is used to transmit system information contained in the SIB. It supports the dynamic rate adaptation and the HARQ (Hybrid Automatic Repeat-reQuest) mechanism. This channel is mapped in the PDSCH.

The MCH transports the multicast traffic data and the associated control data. It is mapped in the PMCH.

The RACH (Random Access CHannel) does not transport logical channels. It is used by the mobile for random access when the mobile is not known to the eNode B entity. It can also be used when the mobile wishes to transmit in the PUSCH (Physical Uplink Shared CHannel) or the PUCCH (Physical Uplink Control CHannel) and when no resource is allocated. This channel is mapped in the PRACH (Physical Random Access CHannel).

The UL-SCH is the main channel in the uplink. It transports the logical signaling (DCCH and CCCH) and traffic (DTCH) channels. It supports dynamic rate adaptation and the HARQ mechanism. This channel is mapped in the PUSCH.

5.1.2.2.3. The RRC protocol

The RRC protocol concerns the signaling exchanged between the mobile and the eNode B entity. The procedures are similar to those described for the UMTS network. They refer to the following points:

– the transmission of system information;

– the establishment of the RRC connection: an RRC connection is indispensable for NAS signaling exchange between the mobile and the MME;

– security activation: the procedure consists of implementing the encryption and integrity control mechanisms for control and traffic flows;

– radio bearer management procedure refers to the establishment, reconfiguration and release of the bearer. It includes the configuration of the ARQ (Automatic Repeat reQuest) mechanisms of the RLC and HARQ protocol of the MAC protocol. It also allows for the configuration of semi-permanent scheduling rules for services such as voice over IP;

– measurement control: the eNode B entity can start measurements at mobile level, carry them out periodically or on demand in order to prepare the handover;

– the handover control procedure allows the change of cell to be carried out between two eNode B (intra-system handover); or between an eNode B and a BTS (for a handover to the GSM/GPRS network) or a Node B (for a handover to a UMTS network).

With regards to the radio resource, the mobile can be in two operational states: the idle state (RRC Idle State) or the connected state (RRC Connected State).

In the idle state, the mobile is not known to the eNode B entity. It stays in this state until the time when the RRC connection procedure is triggered. This triggering is initialized by the mobile when it wishes to transmit data or upon receiving a paging.

In the connected state, the mobile can transmit and receive control and traffic data. The mobile is allocated a C-RNTI (Cell Radio Network Temporary Identity) identifier belonging to the cell. This identifier is used to allocate the PDCCH (Physical Downlink Control CHannel) to the mobile in the downlink.

5.1.2.2.4. The PDCP protocol

The PDCP (Packet Data Convergence Protocol) is responsible for the compression of ROHC (RObust Header Compression) headers, data security and delivery of the data in sequence during a handover.

Security is based on a hierarchy of keys at several levels that allow for the use of separate keys in the access and core networks, host and visitor.

The keys of the first level of CK (Ciphering Key) encryption and IK (Integrity Key) integrity are only visible to the mobile and HSS entity.

At mobile and HSS entity level, the key of the second level K_{ASME} (Access Security Management Entity Key) is derived from the CK and IK, and is transmitted to the MME by the HSS entity.

At mobile and MME level, different keys are derived from the K_{ASME} in order to create third-level keys:

– the CK_{NAS} key used for the encryption of NAS signaling;

– the IK_{NAS} key used for NAS signaling integrity;

– the K_{eNB} key transferred to the eNode B entity.

At mobile and eNode B entity level, different keys are derived from the K_{eNB} in order to create fourth-level keys:

– the $CK_{eNB\text{-}RRC}$ used for encryption of RRC signaling;

– the $IK_{eNB\text{-}RRC}$ used for RRC signaling integrity;

– the $CK_{eNB\text{-}UP}$ used for the encryption of traffic data.

5.1.2.2.5. The RLC protocol

The RLC protocol provides radio link control between the mobile and the eNode B entity for control and traffic data and signalling for this control.

The mobile can simultaneously activate several RLCs, which operate in three modes: the acknowledged mode, the unacknowledged mode and the transparent mode. For the transparent mode, no header is added to the data provided by the PDCP layer.

The RLC protocol carries out the following operations:

– error correction via the ARQ mechanism, solely for the acknowledged mode;

– concatenation, segmentation and reassembly of the PDCP data in acknowledged or unacknowledged mode;

– resegmentation of the RLC data in the acknowledged mode;

– resequencing of received data in the acknowledged or unacknowledged mode;

– detection of duplicated data in the acknowledged or unacknowledged mode;

– protocol error detection and reestablishment of the RLC protocol.

5.1.2.2.6. The MAC protocol

The MAC layer is responsible for the multiplexing of RLC data in the transport blocks, resource allocation via a scheduling mechanism and error management and correction via the HARQ mechanism.

Scheduling defines the modulation or coding scheme to be applied to the transport block for each mobile on the basis of the transmission conditions for the radio channel.

Scheduling also determines the block to be transmitted in the event of an incremental redundancy of the HARQ mechanism.

The retransmission mechanism is of the “Store and Forward” type. The transmission of a data block is conditioned upon receiving the acknowledgement from the previous block. This process does not allow for several consecutive TTIs to be used, which leads to a rate loss.

In the downlink, resolving this problem involves establishing several HARQs for the same user. When one of these awaits acknowledgement from a sent data block, the scheduling can order the transmission of the following block to another HARQ.

5.1.2.3. *The S1−MME interface*

The S1−MME interface supports the S1-AP signaling exchanged between the eNode B entity and the MME.

The MME initializes the paging procedure by sending a S1-AP message to all cells belonging to the TA (Tracking Area) in which the mobile is registered. The mobile's response is sent in a NAS message that the eNode B entity transfers to the MME.

The establishment of the initial context allows the eNode B entity to quickly toggle the idle state to the connected state. The mobile context contains indications such as the context of the bearer, the security context, roaming restrictions and mobile capabilities. This procedure is initialized by the MME in coordination with the attachment or location procedure.

Bearer management is responsible for the establishment, modification and release of resources allocated to the mobile. This procedure is initialized by the MME, with the exception of the release, which can be activated by the eNode B entity.

The preparation and execution procedure of the handover is necessary for inter-system or intra-eUTRAN handover, when the X2 interface is unavailable. When the X2 interface is present, the target eNode B entity transmits a S1-AP message to the MME to alert it that the mobile has been transferred to a new cell.

5.1.2.4. *The X2 interface*

The X2 interface connects the eNode B entities. The X2 interface control plane uses the X2-AP (Application Part) protocol for signaling requirements. The traffic plane uses the GTP-U protocol to transfer IP packets.

The X2-AP protocol supports common and dedicated procedures. An example of a common procedure is the load indication. The dedicated procedures concern mobiles, such as the handover, for example.

The handover procedure is initialized by the source eNode B entity by sending an X2-AP message. The target eNode B entity reserves the radio resources and returns an X2-AP acknowledgement message to the source entity. The acknowledgement message contains the handover command to be transmitted to the mobile, which provides the characteristics of the radio interface. The target entity also communicates the IP address to which the traffic must be transferred on the X2 interface during the handover phase.

The resource release procedure is initialized when the handover has been successful. The target entity indicates to the source that the data transfer must be interrupted and that the radio resources must be released.

The congestion indication procedure is implemented when the interference between the neighboring cells functioning on the same frequency is too great. The eNode B entities agree on the set of sub-carriers to use in the recovery area between two adjacent cells.

5.2. The radio interface

The description of the radio interface is restricted to the physical layer. Figure 5.7 provides a summary of the functions fulfilled by the different layers.

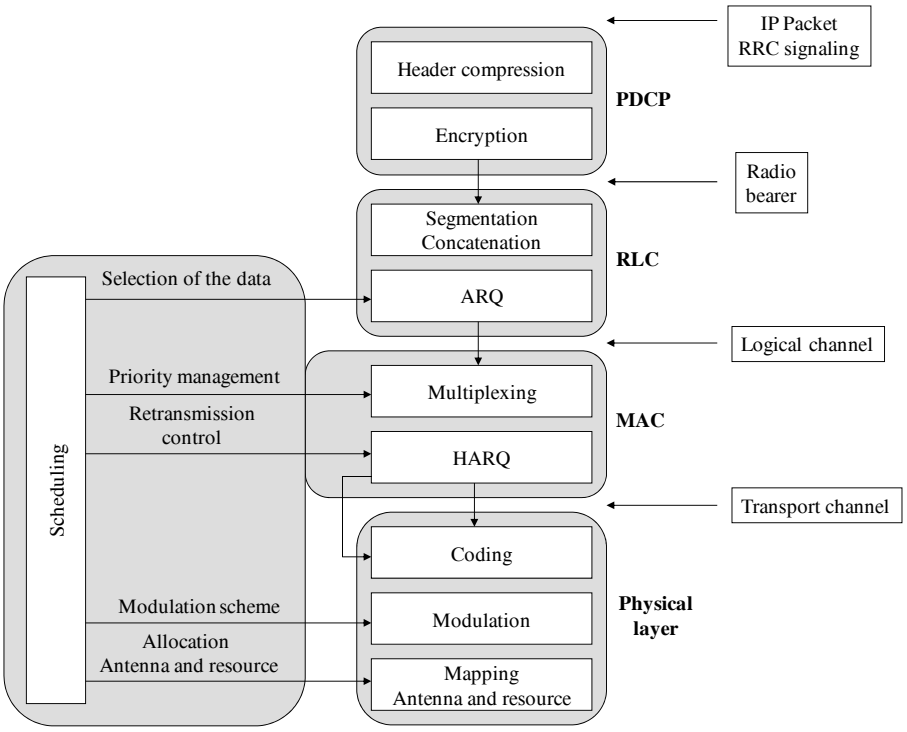


Figure 5.7. *The functions of the radio interface*

5.2.1. *Antenna system*

There are four ways of using the radio channel. It is to be noted that the term "input" applies to the input of the radio channel and the term "output" to the output of the same channel.

The SISO (Single Input Single Output) mode is the basic signal propagation mode for which one transmitting antenna and one receiving antenna are used (Figure 5.8).

The SIMO (Single Input Multiple Output) mode is characterized by the use of one transmitting antenna and several receiving antennas (Figure 5.8). The SIMO mode is often designated as the diversity reception. The transmission rate is identical to the SISO mode. The phase combination of the different signals received, however, allows for improvement of the signal-to-noise ratio.

The MISO (Multiple Input Single Output) mode involves several transmitting antennas and one receiving antenna (Figure 5.8). The MISO mode is often designated as the transmit diversity. The same signal is transmitted on both antennas, but with coding that allows the receiver to identify the transmitters. Like the SIMO mode, the MISO mode improves the signal-to-noise ratio.

The MIMO (Multiple Input Multiple Output) mode uses several transmitting and receiving antennas (Figure 5.8). It improves the rate by authorizing the transmission of different signals on the same frequency at the same time.

Seven antenna systems are defined for the downlink:

– the SIMO mode;

– the MISO mode;

– the MIMO mode without precoding, open loop space-division multiplexing;

– the MIMO mode with precoding, closed loop space-division multiplexing. Precoding allows for the power transmitted and the signal phase to be defined;

– the multi-user MIMO mode with specific precoding for each user;

– the MISO mode with a directional antenna, the beam pointed in the mobile's direction;

– the MISO mode with a directional antenna is different to the previous case because its uses an additional antenna that transmits a reference signal dedicated to the mobile.

Three antenna systems are defined for the uplink:

– the SIMO mode;

– the single-user MIMO mode, where each mobile is equipped with two antennas, which allows the user to double the rate. This system is disadvantageous in terms of cost, size and battery life;

– the multi-user MIMO mode, where each mobile is equipped with a single antenna that in no way modifies the mobile. The different transmitting antennas are those of different mobiles. The remoteness of the mobiles, however, impedes the use of optimized coding.

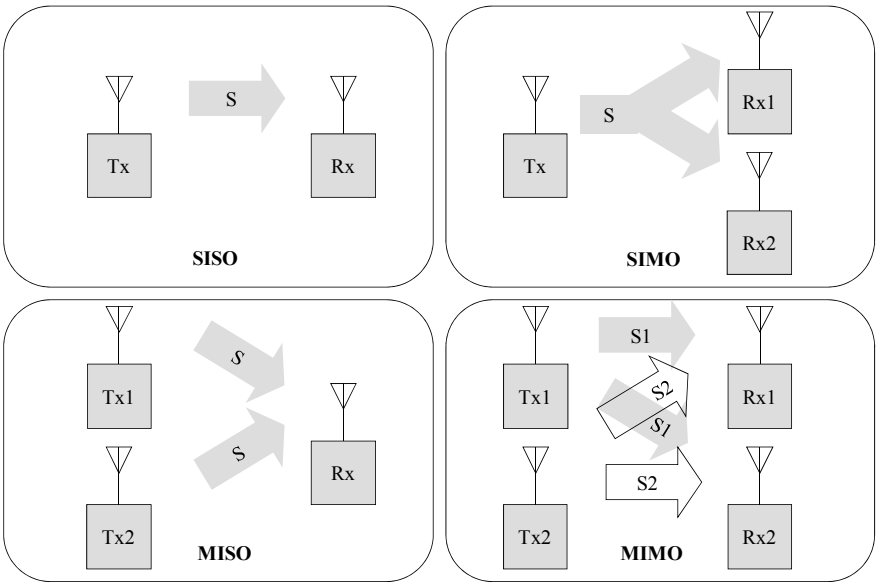


Figure 5.8. *The different antenna systems*

5.2.2. *Access mode*

The downlink uses the OFDMA (Orthogonal Frequency Division Multiple Access) mode in the OFDM (Orthogonal Frequency Division Multiplexing) system, which consists of several orthogonal sub-carriers. Each sub-carrier is modulated by part of the data.

In practice, the OFDM signal is generated by applying an IFFT (Inverse Fast Fourier Transform) to the data to be transmitted. The data are mapped for a user on M points of the IFFT function, each point corresponding to a sub-carrier (Figure 5.9).

The OFDM system has the advantage of being resistant to fading of the signal linked to multiple paths and allows the receiver to function more easily. It does, however, have the inconvenience of generating a signal with a variable peak power.

The OFDMA mode allows for bandwidth sharing between several users. Each user is allocated a time and frequency resource (a number of sub-carriers).

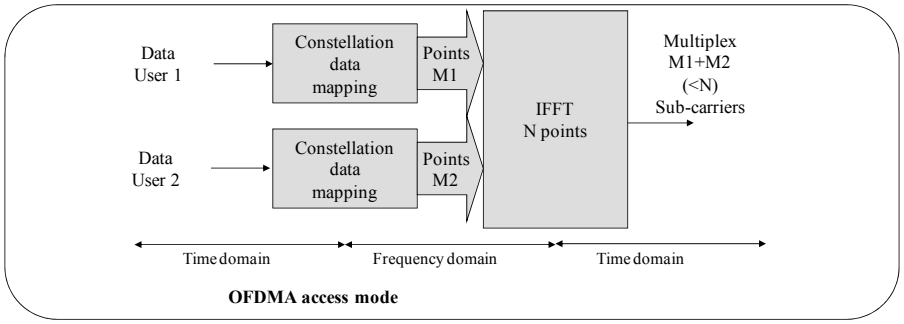


Figure 5.9. *The generation of signals in OFDMA mode*

The uplink uses the SC-FDMA (Single-Carrier Frequency Division Multiple Access) mode, which allows frequency-division multiplexing of several users to be carried out.

In practice, the signal is generated by applying a DFT (Discrete Fourier Transform) to the data in the first instance, then an IFFT in the second instance.

The user's data are mapped in the constellation of the modulation that is retained. Both waveforms obtained from the I and Q channels are applied to the DFT function, which generates M points.

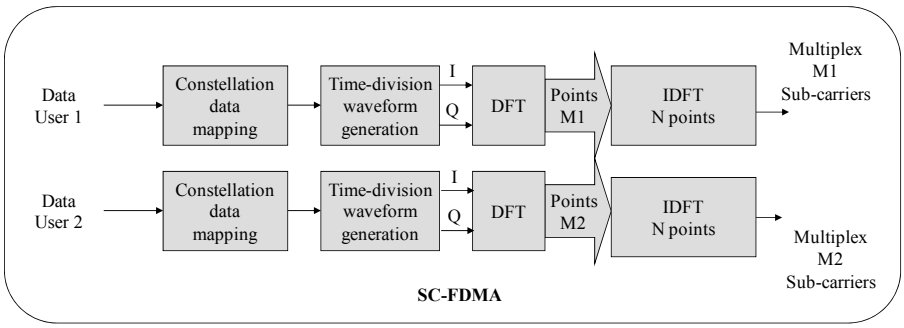


Figure 5.10. *The generation of signals in SC-FDMA mode*

The M points of the DFT function feed the IFFT function. The structure of the resulting signal is similar to that obtained in the OFDMA mode.

The SC-FDMA mode, unlike the OFDMA mode, has the advantage of having a constant peak power for mobiles. This allows for optimization of the conception of the mobile's transmit amplifier. The transmission bearer in both directions uses matched bandwidths in the FDD (Frequency Division Duplex) mode or in a single bandwidth in TDD mode.

The spectrum signal is made up of sub-carriers with a separation 15 kHz. The number of sub-carriers depends on the bandwidth of the radio channel. It defines the size (value of N) of the IFFT function (Table 5.1).

Width of the frequency band	1.4 MHz	3 MHz	5 MHz	10 MHz	15 MHz	20 MHz
Number of sub-carriers	72	180	300	600	900	1,200
IFFT size	128	256	512	1,024	1,536	2,048

Table 5.1. *Characteristics of the OFDM signal*

Table 5.2 specifies the bands that can be used for the radio interface in FDD and TDD mode. These are divided between different continents:

– Europe and Asia (including Japan and China): bands 1, 3, 7 and 8 in FDD and bands 33 (except for Japan), 34, 38 (except for Asia) and 40 in TDD;

– America: bands 2, 4, 5, 10, 12, 13 and 14 in FDD;

– Japan: bands 6, 9 and 11 in FDD;

– China: band 38 in TDD.

FDD mode							
Band	1	2	3	4	5	6	7
Uplink (MHz)	1920-1980	1850-1910	1710-1785	1710-1755	824-849	830-840	2500-2570
Downlink (MHz)	2,110-2,170	1,930-1,990	1805-1880	2110-2155	869-894	875 885	2620-2690

Table 5.2. *The frequency bands in FDD and TDD mode*

FDD mode							
Band	8	9	10	11	12	13	14
Uplink (MHz)	880-915	1750-1785	1710-1770	1428-1463	698-716	777-787	788-798
Downlink (MHz)	925-960	1845-1880	2110-2170	1476-1501	728-746	746-756	758-768

TDD mode								
Band	33	34	35	36	37	38	39	40
Uplink/Downlink (MHz)	1900-1920	2010-2025	1950-1910	1930-1990	1910-1930	2570-2620	1880-1920	2300-2400

Table 5.2. *(continued) The frequency bands in FDD and TDD mode*

The same frequency band can be used in each cell covered by the eNode B radio station. In order to avoid interference, the following is set up (Figure 5.11):

– the entire spectrum is used in the central area of the cell, for which the interference created by the neighboring cells is weak;

– part of the spectrum is used in the peripheral area of the cell, which allows interference from the neighboring cells to be removed.

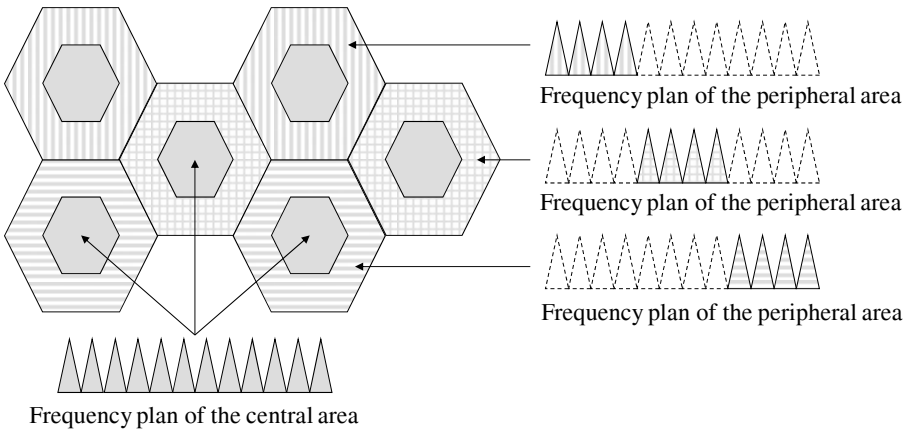


Figure 5.11. *The frequency plan of cells*

5.2.3. *Frame structure*

The same frame structure is used for both directions of transmission. Two frame structures are defined according to the FDD or TDD mode. The durations are expressed in multiples of the factor Ts (Ts = 1/15,000 * 2,048).

The type 1 structure defined for the FDD mode has a duration of 10 ms (= 307,200 * Ts) and contains 10 sub-frames (Figure 5.12). Each sub-frame consists of two time-slots. Each time-slot consists of three, six or seven symbols. A symbol contains a number of sub-carriers, depending on the width of the frequency band of the radio channel.

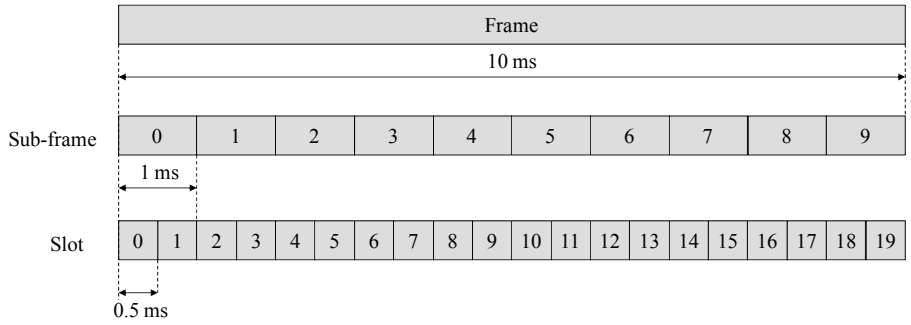


Figure 5.12. *The structure of the frame in FDD mode*

The type 2 structure defined for the TDD mode also has a duration of 10 ms. It contains two half-frames of 5 ms each (Figure 5.13). Each half-frame carries eight time-slots and three specific fields:

– a DwPTS (Downlink Pilot Time-Slot);

– an UpPTS (Uplink Pilot Time-Slot);

– a moment of silence, GP (Gap Period), between the two proceeding time-slots.

For the uplink, the signals transmitted by the different mobiles must be time-divisionally aligned to the interior of a sub-frame. The mobiles must be synchronized by the eNode B entity, which tells them the time-advance to be applied.

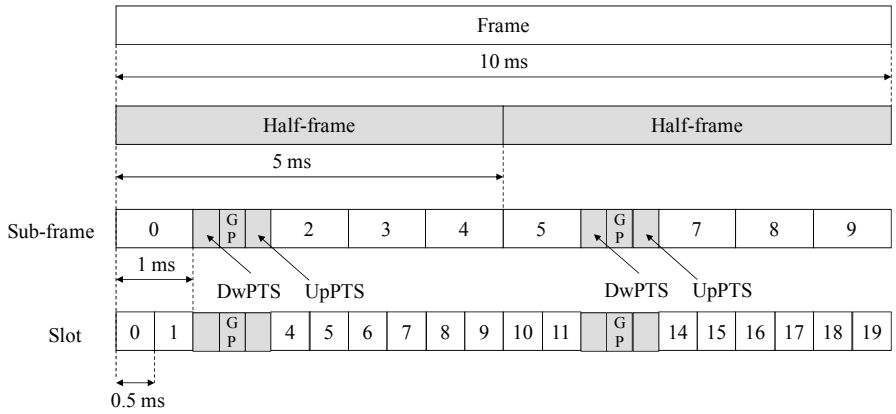


Figure 5.13. *The structure of the frame in TDD mode*

The sub-frames are allocated to the traffic for the uplink and downlink, or for the particular fields according to various configurations (Table 5.3):

– sub-frames 0 and 5 are always allocated to traffic in the downlink;

– sub-frame 1 is always allocated to three specific fields;

– sub-frame 2 is always allocated to the traffic in the uplink;

– sub-frame 6 is allocated to three specific fields for a periodicity of 5 ms.

Configuration	**Periodicity**	**Number of the sub-frame**									
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	5 ms	D	S	U	U	U	D	S	U	U	U
1	5 ms	D	S	U	U	D	D	S	U	U	D
2	5 ms	D	S	U	D	D	D	S	U	D	D
3	10 ms	D	S	U	U	U	D	D	D	D	D
4	10 ms	D	S	U	U	D	D	D	D	D	D
5	10 ms	D	S	U	D	D	D	D	D	D	D
6	5 ms	D	S	U	U	U	D	S	U	U	D

D – downlink;
U – uplink;
S − special (specific fields)

Table 5.3. *Configuration of the TDD frame*

Figure 5.14 describes the structure of the TDD frame for configuration 1.

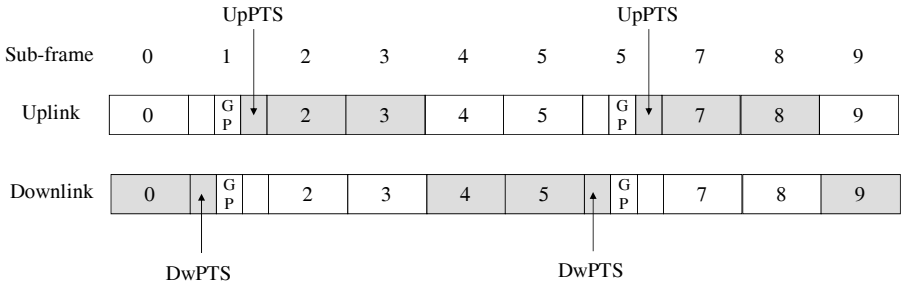


Figure 5.14. *The structure of the TDD frame – configuration 1*

The introduction of a guard time between the symbols allows for elimination of inter-symbol interference. Each OFDM symbol is cyclically extended in the guard time by copying the end of the symbol for the cyclic prefix (see Figure 5.15 and Table 5.4).

The extended cyclic code is essentially used in cases where spreading of the delay between different reflected signals is significant, which is the case for cells with a large diameter (Table 5.4).

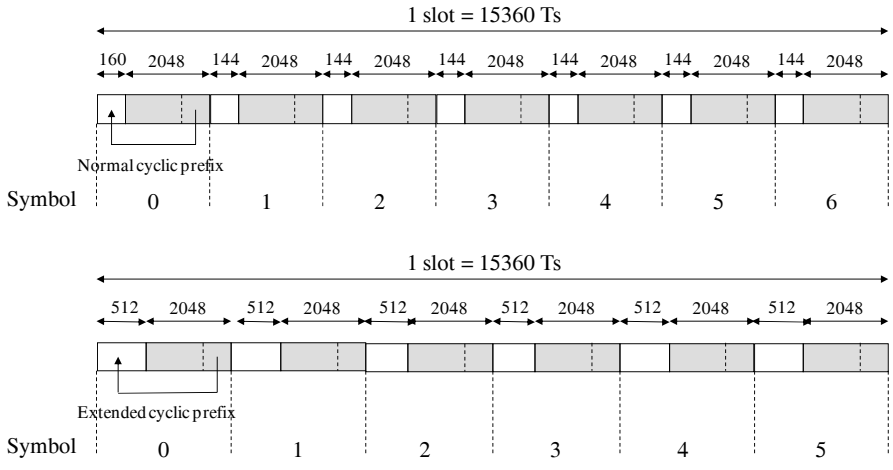


Figure 5.15. *Structure of the time-slot*

Downlink		**Length of the cyclic prefix**
Normal cyclic prefix	Δf (1) = 15 kHz	160 * Ts for l (2) = 0 and 144 * Ts for l = 1, 2,..., 6
Extended cyclic prefix	Δf = 15 kHz	512 * Ts for l = 0, 1,..., 5
	Δf = 7.5 kHz	1,024 * Ts for l = 0, 1, 2
Uplink		**Length of the cyclic prefix**
Normal cyclic prefix		160 * Ts for l = 0 and 144 * Ts for l = 1, 2,..., 6
Extended cyclic prefix		512 * Ts for l = 0, 1, ..., 5

Δf – separation between sub-carriers;
l – the number of the symbol in the slot

Table 5.4. *Length of the cyclic prefix*

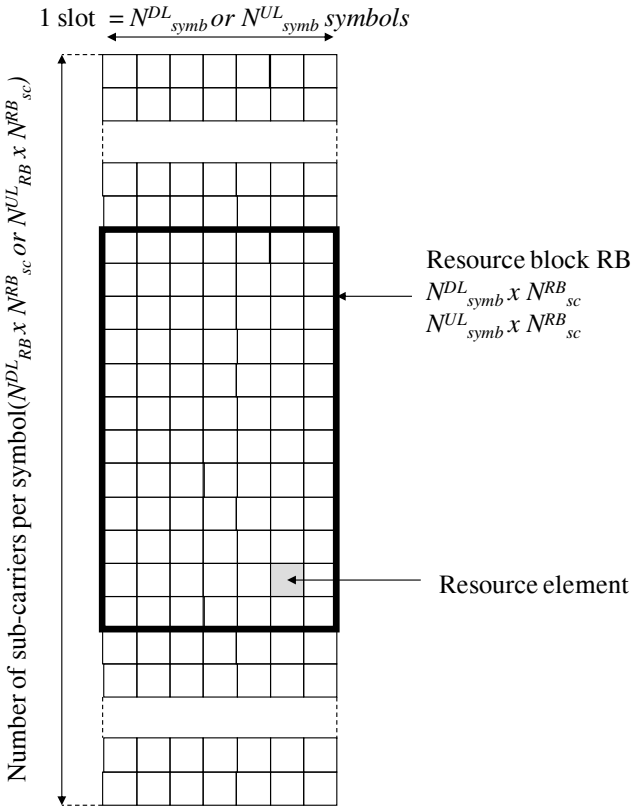


Figure 5.16. *Structure of the RB*

A resource element corresponds to the smallest unit that can be allocated to a physical signal (Figure 5.16). It corresponds to a symbol in the time domain and to a sub-carrier in the frequency domain.

The RB (Resource Block) is the smallest unit allocated to a user (Figure 5.16). It corresponds to a 0.5 ms (one slot) in the time domain and to 180 Hz in the frequency domain. The number of sub-carriers and symbols per RB depends on the spacing between the sub-carriers and the size of the cyclic prefix (Table 5.5).

Downlink		N^{RB}_{sc}	N^{DL}_{symbol}
Normal cyclic prefix	Δf = 15 kHz	12	7
Extended cyclic prefix	Δf = 15 kHz		6
	Δf = 7,5 kHz	24	3
Uplink		N^{RB}_{sc}	N^{UL}_{symbol}
Normal cyclic prefix		12	7
Extended cyclic prefix		12	6

N^{RB}_{sc} – *number of sub-carriers for a RB;*
N^{DL}_{symbol} – *number of symbols per slot for the downlink;*
N^{UL}_{symbol} – *number of symbols per slot for the uplink*

Table 5.5. *Parameters of the RB*

Table 5.6 provides the number of RBs in a time-slot, according to the bandwidth.

Bandwidth (MHz)	1	3	5	10	15	20
Bandwidth used	1.08	2.7	4.5	9	13.5	18
Number of RBs	6	15	25	50	75	100

Table 5.6. *Number of RBs per time-slot*

5.2.4. *The signals and physical channels*

The radio interface has physical signals and channels. The physical signals are used to synchronize the system, to identify cells and to estimate the radio channel. The physical channels are used to transport the traffic and control data from the upper layers.

5.2.4.1. *The downlink*

The signals and physical channels in the downlink are specified in Table 5.7.

Physical signals		
Primary Synchronization Signal	PSS	Synchronization of the half-frame and identification of the cell (index of the group)
Secondary Synchronization Signal	SSS	Synchronization of the frame and identification of the cell (index in the group), the FDD or TDD mode and the length of the prefix
Reference signal		Demodulation bearer (frequency synchronization)
Physical channels		
PBCH	Physical Broadcast CHannel	System information of the cell
PDCCH	Physical Downlink Control CHannel	Signaling concerning the allocation of the data received in the downlink and the scheduling of data to be transmitted in the uplink
PCFICH	Physical Control Format Indicator CHannel	Number of OFDM symbols allocated to the PDCCH
PHICH	Physical HARQ Indicator CHannel	Acknowledgement of the data received from the mobile
PDSCH	Physical Downlink Shared CHannel	Unicast traffic transport channel bearer
PMCH	Physical Multicast CHannel	Multicast traffic transport channel bearer

Table 5.7. *Signals and the physical channels – the downlink*

5.2.4.1.1. The physical reference signal

There are three types of reference signal:

– the reference signal dedicated to a cell, transmitted on antennas 0 to 3;

– the reference signal dedicated to multicast traffic, transmitted on antenna 4;

– the reference signal dedicated to a mobile, transmitted on an additional antenna.

The reference signal dedicated to a cell is generated from a pseudo-random sequence of 31 bits (Gold sequence), whose polynomial generator depends on the number of the time-slot, the number of the OFDM symbol, the identity of the cell and the type of prefix.

The reference signal dedicated to a cell is mapped in four resource elements in each RB, located in the symbols 0 and 3 (1 and 4 respectively) for antennas 0 and 1 (2 and 3 respectively), see Figure 5.17.

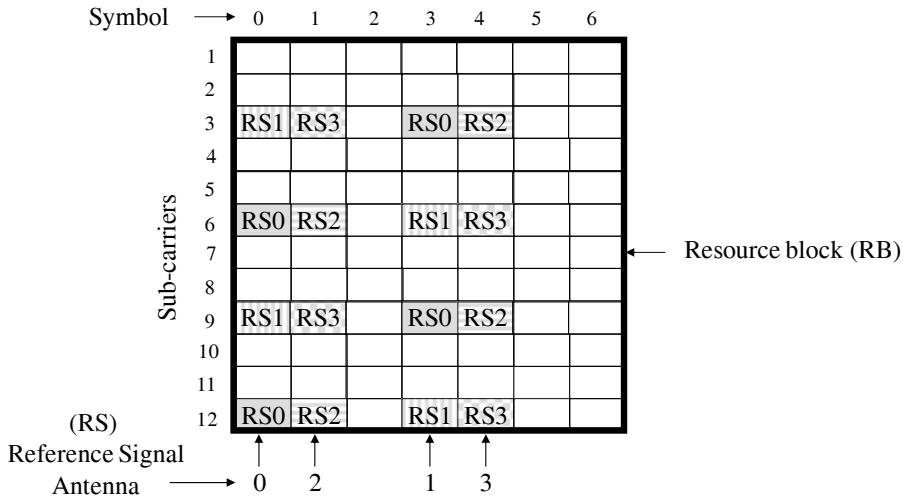


Figure 5.17. *Position of the reference signal dedicated to the cell*

5.2.4.1.2. The PSS physical signal

A cell has an identification that can take 504 values, which are divided into three groups. The PSS (Primary Synchronization Signal) is generated from a Zadoff-Chu sequence that corresponds to the value of the group.

In the FDD mode, the PSS is mapped in the last symbol of slots 0 and 10. The position of the resource elements is given in the following formula:

$$k = n - 31 + (N^{RB}_{dl} * N^{SC}_{rb}) / 2, \text{ with } n = 0, 1, 2, \ldots, 61$$

where:

– k is the number of the sub-carrier;

– N^{RB}_{dl} the number of RBs for the downlink;

– $N^{SC}_{rb\ \text{the}}$ number of sub-carriers in a RB.

The combination of the sequence is the same for both slots, which allows for recovery of the synchronization of the half-frame.

In the TDD mode, the PSS is mapped in the third symbol of sub-frames 1 and 6. The position of the resource elements is given in the following formula:

$$k = n - 31 + + (N^{RB}_{dl} * N^{SC}_{rb}) / 2, \text{ with } n = -5,-4,\ldots,-1, 62, 63,\ldots, 66.$$

5.2.4.1.3. The physical SSS

The physical SSS (Secondary Synchronization Symbol) corresponds to two sequences of 31 interleaved bits, which are used to detect the identification of the cell in the group. Each sequence is scrambled by a code defined by the PSS.

In the FDD mode, the SSS is mapped in the penultimate symbol of slots 0 and 10. The combination of both 31 bit symbols is different for each slot, which allows for recovery of the frame synchronization.

The physical SSS must also allow for detection of the type of cyclic prefix (normal or extended). Detection is carried out blindly and two transitions by the FFT function are necessary for this when receiving.

In the TDD mode, the SSS is mapped in the last symbol of slots 1 and 11. The position of the resource elements is given in the following formula:

$$k = n - 31 + (N^{RB}_{dl} * N^{SC}_{rb}) / 2, \text{ with } n = 0, 1, 2, \ldots, 61$$

5.2.4.1.4. The PCFICH

The PCFICH (Physical Control Format Indicator CHannel) contains two bits of CFI (Control Format Indicator) information and uses coding with a rate equal to 1/16. The information is transmitted in 16 resource elements of the sub-frame's first symbol. The 2 bits of each resource element correspond to a QPSK modulation constellation (Figure 5.18).

The position of the resource elements is spread over four groups and depends on the identification of the cell for interference between the cells to be avoided (Figure 5.18).

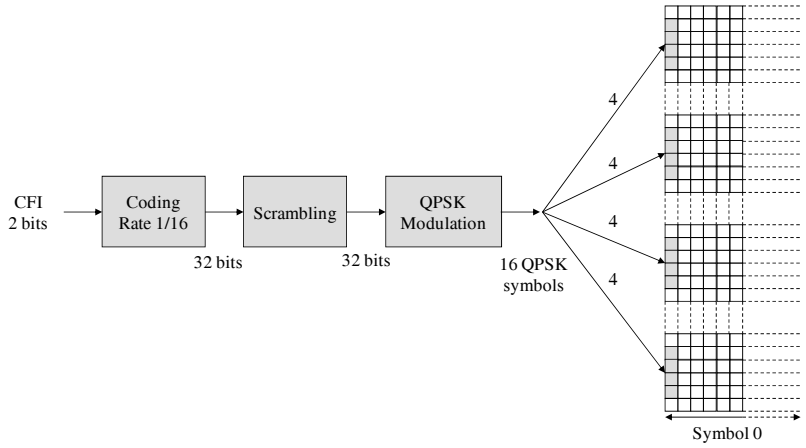


Figure 5.18. *The PCFICH*

5.2.4.1.5. The PHICH

The PHICH transports the HI (HARQ Indicator) information, which indicates an ACK (ACKnowledgment) or a NACK (Negative ACKnowledgment) of the data received for the uplink.

In FDD mode, the RB received by the eNode B entity must be acknowledged four sub-frames later. In TDD mode, the rule is similar and the acknowledgement must be able to be applied to several RBs in view of the frame configuration.

This information is repeated three times and uses a Walsh spread sequence in order to multiplex several responses to the mobiles and to improve resistance to errors (Figure 5.19).

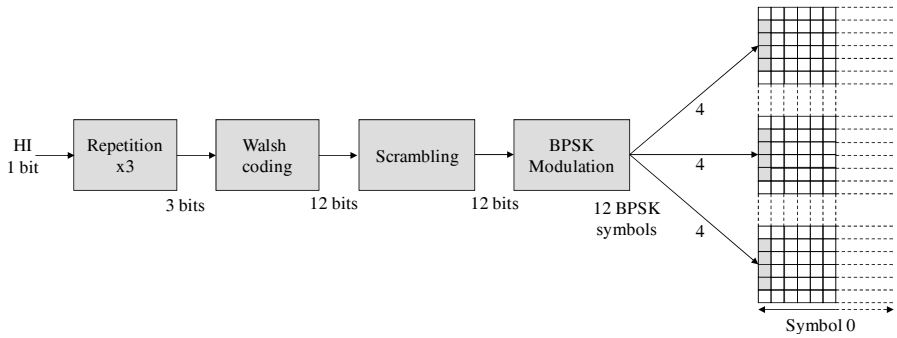


Figure 5.19. *The PHICH*

A BPSK (Binary Phase-Shift Keying) modulation generates 12 symbols transmitted in 12 resource elements located in the first OFDM symbol of the sub-frame. The position of the resource elements is indicated in the PBCH in order to avoid collisions with neighboring cells (Figure 5.19).

5.2.4.1.6. The PBCH

The physical PBCH contains 1,920 bits in the case of a normal prefix or 1,728 bits in the case of an extended prefix. The information is divided into four frames and is located in the first four symbols of time-slot 1. The position of the resource elements is given in the following formula:

$$k = (N^{RB}_{dl} * N^{SC}_{rb}) /2 - 36 + k', \text{ with } k' = 0,1,\ldots,71 \text{ and } l = 0, 1\ldots 3$$

where l is the number of the OFDM symbol in the time-slot.

Figure 5.20 describes the processing operations carried out on the different pieces of system information. As the transport BCH gives no information regarding the number of antennas used by the eNode B entity, this information is obtained from a mask applied to the CRC (Cyclic Redundancy Check).

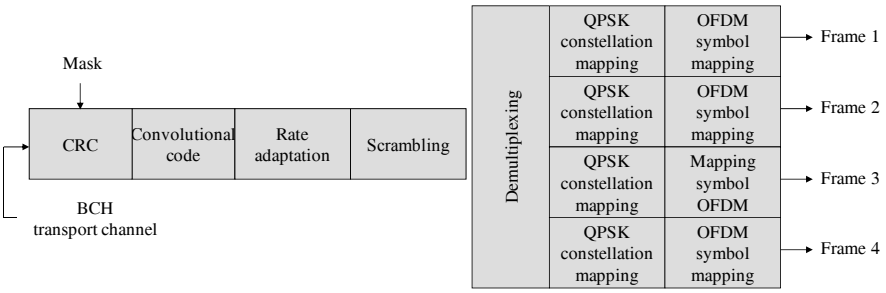


Figure 5.20. *The PBCH*

5.2.4.1.7. The PDCCH

The PDCCH transports different control information for the DCI (Downlink Control Information) downlink including:

– the allocation of the PDSCH;

– SIB system information;

– paging information;

– the response to an access request;

– the mobile's power level.

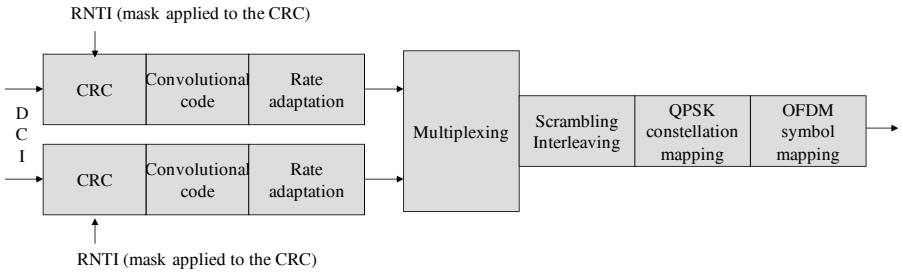


Figure 5.21. *The PDCCH*

The PDCCH is transmitted in the first OFDM symbols of each sub-frame. The number of symbols used is indicated by the PCFICH.

Figure 5.21 describes the processing operations carried out on the different types of control information. For each type of information, a mask based on the RNTI is applied to the CRC, which allows for demultiplexing when receiving.

5.2.4.1.8. The PDSCH

A 24-bit cyclic redundancy code is applied to the data in the transport channel in order to detect residual errors when receiving. The receiver transmits a HARQ ACK in the PUCCH if the data are correct and a HARQ NACK in the opposite case (Figure 5.22).

Segmentation is applied to the data derived from the preceding phase when the size of the data is larger than 6,144 bits. This value corresponds to the maximum size of the turbo code. The segments obtained are all the same size, with the possibility of adding stuffing bits for completion (Figure 5.22).

A turbo code is used to carry out an error correction upon receiving, with a coding rate of 1/3. The rate adaptation function allows for repetition or puncturing of the bits (Figure 5.22).

When segmentation is carried out, the different segments are concatenated before being scrambled by a sequence belonging to the cell.

The data are then mapped in order to obtain the QPSK, 16-QAM or 64-QAM modulation symbols that will be carried out on one, two, three or four antennas. A precoding is applied to the I and Q channels according to the type of system used by the retained antenna (Figure 5.22).

The PDSCH holds the unused resource elements.

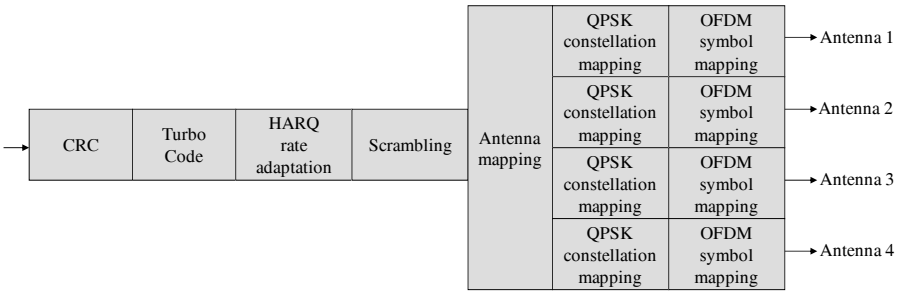


Figure 5.22. *The PDSCH*

Table 5.8 specifies the maximum rates of the PDSCH on the basis of the following hypotheses:

– the 64 QAM modulation is used;

– a symbol is allocated to the control channels;

– the coding rate is equal to 1;

– the calculation is carried out that does not take the reference signals (PSS and SSS) and the PBCH into account.

Length of the frequency band	**Number of antennas**		
	1	**2**	**4**
1.4 MHz	5.4 Mbps	10.4 Mbps	19.6 Mbps
3 MHz	13.5 Mbps	25.9 Mbps	50.0 Mbps
5 MHz	22.5 Mbps	43.2 Mbps	81.6 Mbps
10 MHz	45 Mbps	86.4 Mbps	163.2 Mbps
15 MHz	67.5 Mbps	129.6 Mbps	244.8 Mbps
20 MHz	90.0 Mbps	172.8 Mbps	326.4 Mbps

Table 5.8. *The rates of the PDSCH*

5.2.4.1.9. Multiplexing of the signals and physical channels

Figure 5.23 describes a multiplexing structure of the (PSS and SSS) signals and the physical channels (PDCCH, PDSCH and PBCH).

The allocation of resources obeys the following rules:

– the physical signals have priority, as opposed to the physical channels;

– the physical channels PCFICH and PHICH have priority, as opposed to the PDCCH;

– the PBCH has priority as opposed to the PDSCH;

– the control channels (PHICH, PCFICH and PDCCH) and the traffic channels (PDSCH) occupy different symbols in the time-slot.

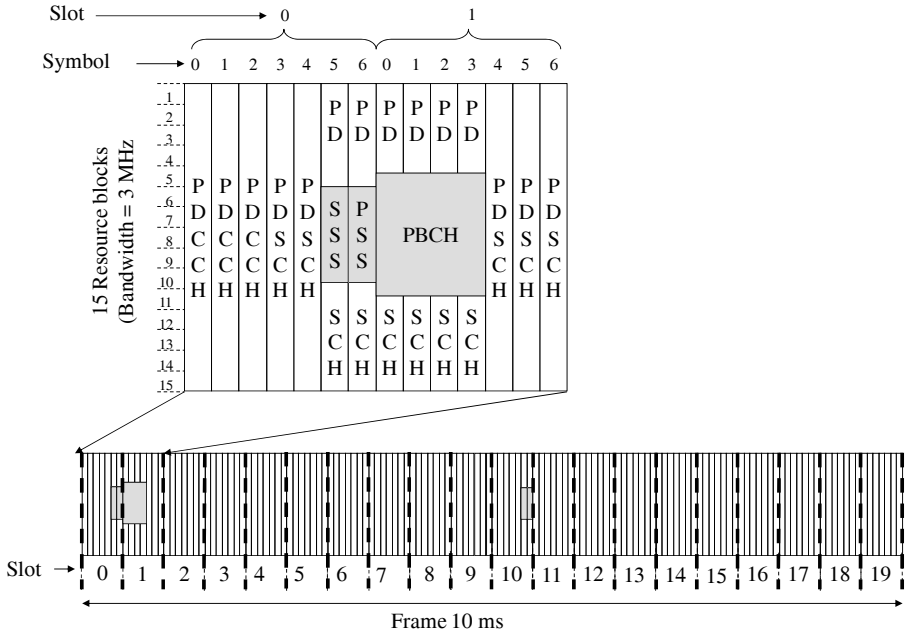


Figure 5.23. *Multiplexing of the signals and physical channels*

It is to be noted that the physical PSS and SSS and the PBCH occupy the same frequency band, whatever the length of radio channel band (36 resource elements on both sides of the central frequency). This allows the mobile (thanks to the PSS and SSS channels) to synchronize and recover the length of the frequency band (thanks to the PBCH), see Figure 5.24.

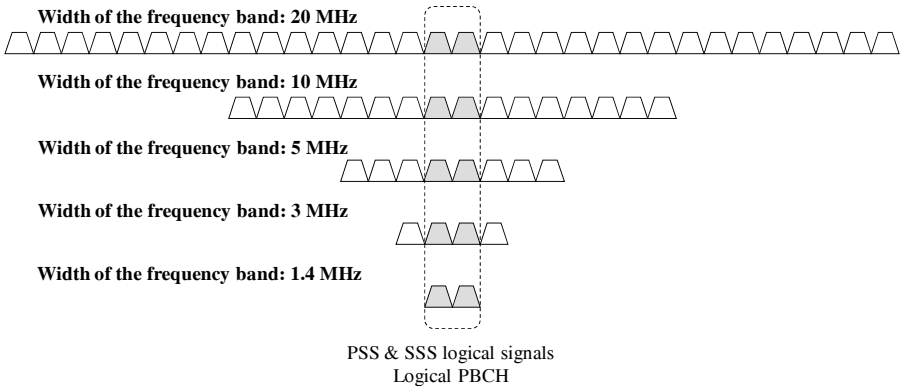


Figure 5.24. *The positioning of PSS and SSS signals and of the PBCH*

5.2.4.2. *The uplink*

The signals and physical channels in the uplink are indicated in Table 5.9.

Physical signals		
DRS	Demodulation Reference Signal	Bearer for demodulation
SRS	Sounding Reference Signal	Assessment of the radio channel
Physical channels		
PRACH	Physical Random Access CHannel	Random access to the radio resource
PUCCH	Physical Uplink Control CHannel	Signaling concerning acknowledgement of data received in the downlink, the quality of signal received and the resource request for the downlink
PUSCH	Physical Uplink Shared CHannel	The unicast traffic transport channel bearer

Table 5.9. *The signals and physical channels – uplink*

5.2.4.2.1. The physical reference signal

The reference signal is constructed from a Zadoff-Chu sequence, whose characteristic is to optimize the value of self- and inter-correlation. Several DRSs (Demodulation Reference Signals) or SRSs (Sounding Reference Signals) that simultaneously come from different mobiles are multiplexed with the help of these sequences.

The position of DRS when attached to the PUCCH depends on the type of PUCCH and the cyclic prefix.

The position of the DRS when associated with the PUSCH occupies the fourth symbol (third symbol, respectively), when the normal cyclic prefix is used (extended, respectively).

The SRS is transmitted in the last symbol of the sub-frame and uses the entire spectrum, with a periodicity varying from 2 ms (in both of the two sub-frames) to 160 ms (all 16 frames).

5.2.4.2.2. The PUCCH

The PUCCH is used to transport the control information only when a resource on the PUSCH is not allocated to the mobile. In the opposite case, the PUSCH is used to transport control data.

Several mobiles can use the same RB. The multiplexing of different mobiles is obtained by orthogonal sequences.

The PUCCH is transmitted to the two extremities of the spectrum. The format type depends on the type of information that is supported (Table 5.10).

Format of the PUCCH	Modulation	Number of bits per sub-frame	Use
1	Not applicable	Not applicable	Scheduling request
1a	BPSK	1	ACK/NACK
1b	QPSK	2	ACK/NACK
2	QPSK	20	CQI
2a	QPSK + BPSK	21	CQI + ACK/NACK
2b	QPSK + BPSK	22	CQI + ACK/NACK

Table 5.10. *Format of the PUCCH*

For the 1× format, the PUCCH is transmitted in four symbols of a RB (symbol 0, 1, 5 and 6), the three others being allocated to the DRS associated with the physical channel.

For the 2× format, the PUCCH is transmitted in five symbols of a RB (symbol 0, 2, 3, 4 and 6), the two others being allocated to the DRS associated with the physical channel.

The PUCCH transports the quality indications concerning the downlink:

– CQI (Channel Quality Indicator): this parameter indicates the modulation type and the coding rate to be applied;

– RI (Rank Indicator): this parameter indicates which row of the antenna to use;

– PMI (Precoding Matrix Indicator): this parameter indicates the precoding values to be applied to the signal.

5.2.4.2.3. The PRACH

A resource of the PRACH occupies six RBs. The position of the physical channel is indicated by the SIB. The PRACH can be absent in a sub-frame or in a frame.

Several mobiles can access the same resource by using different preambles. In each cell, there are 64 preambles based on Zadoff-Chu-type sequences. Access can be made with or without contention.

As the synchronization for the uplink is still not established, the transmission uses a guard period in order to manage the temporal uncertainty. This uncertainty depends on the size of the cell (6.7 μs/km).

The transmission of the preamble, the cyclic prefix and the guard time is carried out over a duration of 1 ms, that is to say that of both symbols, with the following distribution:

– 0.1 ms for the cyclic prefix;

– 0.8 ms for the preamble;

– 0.1 ms for the guard time, which allows the cells to have a 15 km radius.

Three other structures allow the guard time to be increased in order to reach mobiles located 100 km from the eNode B entity. These four structures are operational for the TDD and FDD modes.

A fifth structure is defined solely for the TDD mode. The preamble is transmitted in the UpPTS field rather than in a normal sub-frame. Like the UpPTS field, it is solely transmitted in a sub-frame. The duration of the guard time is shorter than that of the preceding configurations. This structure must therefore be reserved for small cells.

5.2.4.2.4. The PUSCH

The PUSCH occupies the remaining RBs. The processing carried out is similar to that of the downlink.

Table 5.11 indicates the peak rates of the PUSCH calculated on the basis of the following hypotheses:

– the 64 QAM modulation is used;

– the coding rate is equal to 1;

– a single RB is allocated to the PUCCH for the width of the frequency band equal to 1.4 MHz; two RBs for the other frequency bands;

– the calculation is carried out without considering the SRS or the PRACH.

Width of the frequency band	**1.4 MHz**	**3 MHz**	**5 MHz**	**10 MHz**	**15 MHz**	**20 MHz**
Rate (Mbps)	4.3	10.4	17.3	41.5	62.2	82.9

Table 5.11. *The rates of the PUSCH*

5.2.4.2.5. Multiplexing of signals and physical channels

Figure 5.25 describes a multiplexing structure of the signals (DRS and SRS) and the physical channels (PUSCH and PUCCH).

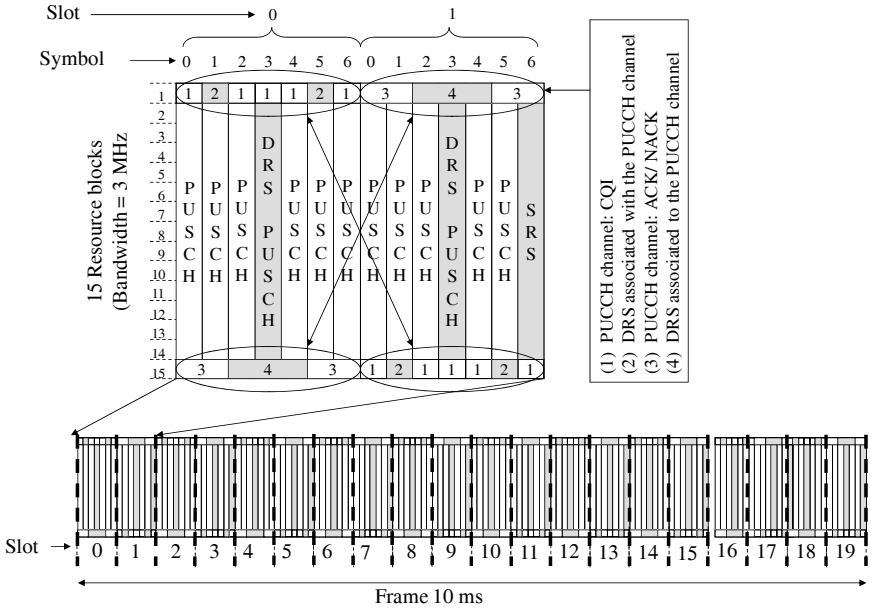


Figure 5.25. *Multiplexing of the signals and physical channels – uplink*

Both PUCCH format types are shown, illustrating the position of the DRS associated with this channel.

5.3. Communication management

5.3.1. *The attachment procedure*

The attachment procedure follows the two following procedures:

– the establishment of the RRC connection between the mobile and the eNodeB entity;

– registration of the mobile close to the MME.

5.3.1.1. *Establishment of the RRC connection*

Establishment of the RRC connection starts via the random access procedure. The random access procedure occurs when the mobile is switched on, when it is in the RRC idle state and when it wishes to establish a session, or when it carries out a location update. The random access implements a procedure with contention. There is a risk of collision between several mobiles, which will have to repeat the request.

The mobile also starts this procedure during a handover or during a loss of synchronization for the uplink. The random access implements a procedure without contention. In the procedure with contention, the mobile transmits the RANDOM ACCESS PREAMBLE containing a temporary identity on the RACH (Figure 5.26).

The RANDOM ACCESS RESPONSE of the eNode B entity contains the temporary identity of the mobile, a C-RNTI, the information of the time-advance and a resource allocation for the uplink (Figure 5.26).

In the procedure without contention, the mobile is already in communication with the eNode B entity. The procedure starts by sending a preamble allocated by the eNode B entity to the mobile (Figure 5.26).

The mobile transmits a RRC CONNECTION REQUEST message to the entity, which can encapsulate a NAS attachment service or a TA location update request message. This message is transmitted in the logical CCCH (Figure 5.26).

The eNode B entity responds with a RRC CONNECTION SETUP message. This message allows the mobile to establish the RRC connection and to set up a resource for the transport of signaling exchanged with the eNode B and MMEs. This message is transmitted in the logical CCCH (Figure 5.26).

The mobile responds with the RRC CONNECTION SETUP COMPLETE message. This message is transmitted in the logical DCCH (Figure 5.26).

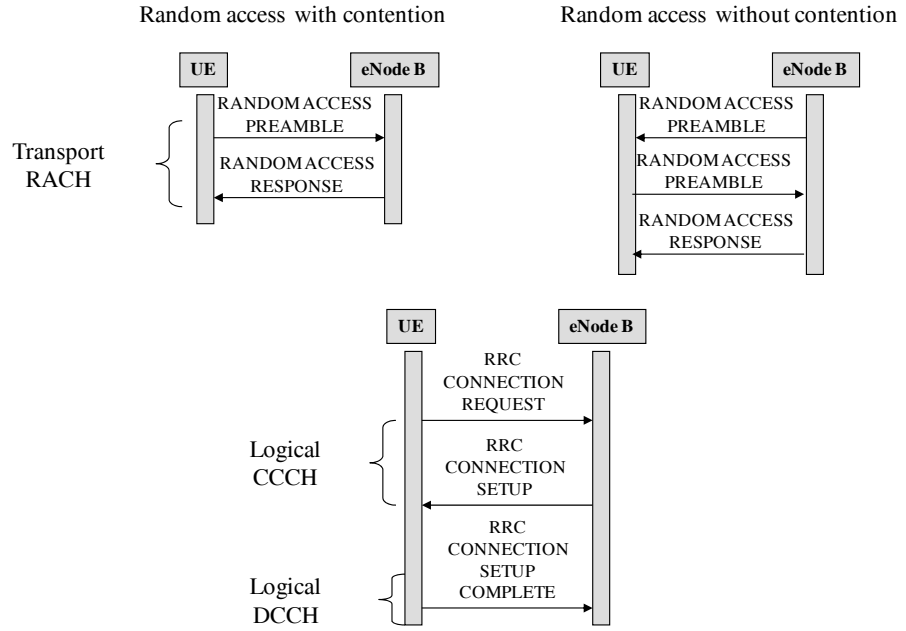


Figure 5.26. *Establishment of a RRC connection*

5.3.1.2. *Registration*

The registration procedure aims to carry out mutual authentication between the mobile and the MME, to register the mobile's location, to allocate a temporary GUTI to it and to establish a default bearer.

The registration procedure is triggered by the mobile when it sends the NAS ATTACH REQUEST message to the eNode B entity containing its IMSI or GUTI, if it knows them (Figure 5.27).

The selection of the MME allocated to the mobile is achieved by the eNode B entity which transfers the NAS ATTACH REQUEST message.

After the authentication procedure identical to that implemented in the UMTS network, the MME updates the mobile's location in the HSS database via the DIAMETER UPDATE LOCATION message (Figure 5.27).

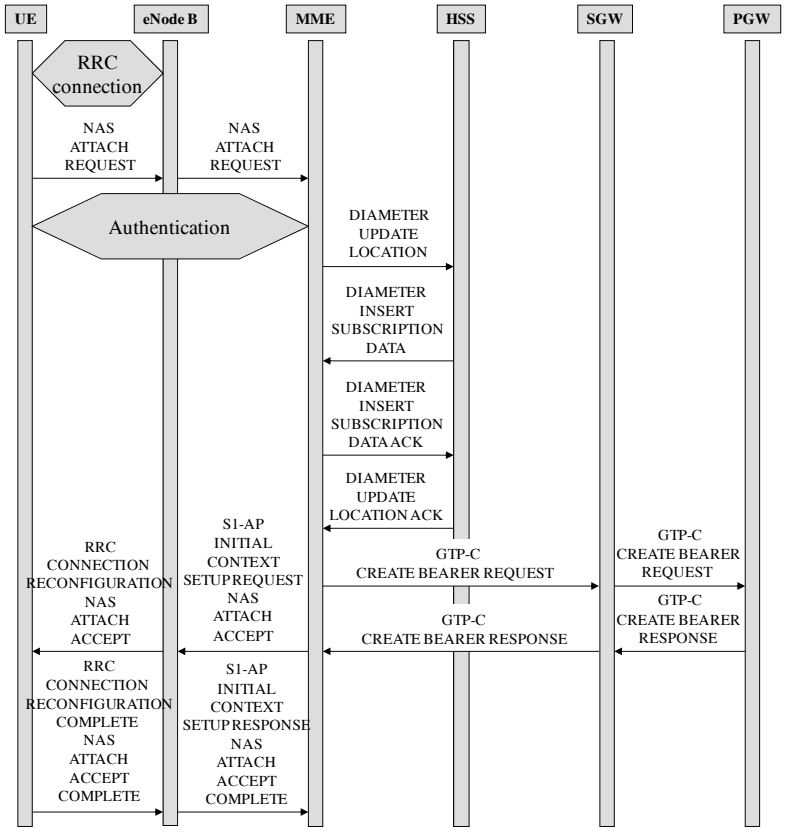


Figure 5.27. *The registration procedure*

In return, the HSS entity provides the MME with the mobile's profile via the DIAMETER INSERT SUBSCRIPTION DATA message (Figure 5.27).

Both DIAMETER messages (INSERT SUBSCRIPTION DATA then UPDATE LOCATION) are acknowledged by the MME and HSS entity, respectively.

The second phase concerns the establishment of the default bearer by exchanging following signaling (Figure 5.27):

– the GTP-C CREATE BEARER REQUEST and CREATE BEARER RESPONSE messages;

– the NAS ATTACH ACCEPT messages containing the GUTI and ATTACH COMPLETE;

– the S1-AP INITIAL CONTEXT SETUP REQUEST and INITIAL CONTEXT SETUP RESPONSE messages, encapsulating the NAS ATTACH ACCEPT and ATTACH COMPLETE messages on the interface between the MME and eNode B entity, respectively;

– the RRC CONNECTION RECONFIGURATION and CONNECTION RECONFIGURATION COMPLETE messages respectively encapsulating the NAS ATTACH ACCEPT and ATTACH COMPLETE messages on the radio interface.

5.3.2. *Location updating*

The mobile decides to precede to a location update when it enters a new cell or when the hold timer has expired. The location update results in the following operations:

– update of the bearer between the SGW entity in charge of the new TA and the mobile; and possibly between the new SGW entity and the PGW entity;

– transfer of the mobile context of the former MME to the new one;

– update of the HSS entity with the IP address of the new MME.

The mobile initializes the location update procedure by sending the NAS TA UPDATE REQUEST message (Figure 5.28).

The eNode B entity determines the identity of the MME from the parameters of the protocol transmitted by the mobile. If this MME is not associated with the eNode B entity, this determines the new MME allocated to the mobile and transfers the NAS UPDATE REQUEST message to it (Figure 5.28).

The new MME determines the identity of the former entity from the GUTI, and contacts MME by sending it the GTP-C CONTEXT REQUEST message. In return, the former MME returns the mobile's context in the GTP-C CONTEXT RESPONSE message (Figure 5.28).

The authentication procedure is performed between the mobile and the new MME, which later acknowledges the transfer regarding the former MME by sending it the GTP-C CONTEXT ACKNOWLEDGE message (Figure 5.28).

The new MME modifies the bearer between the eNode B and SGW entities via an exchange of GTP-C MODIFY BEARER REQUEST and MODIFY BEARER RESPONSE signaling. When the SGW entity is new, the same exchange is carried out between the SGW and PGW entities (Figure 5.28).

The new MME updates the mobile's location with the HSS entity via the exchange of DIAMETER UPDATE LOCATION REQUEST and UPDATE LOCATION ACK messages. The HSS entity proceeds to cancel the mobile information in the former MME (Figure 5.28).

The new entity can thus respond to the mobile via the transmission of the NAS TA UPDATE ACCEPT message containing a new GUTI. This message is acknowledged in return by the mobile via the NAS TA UPDATE COMPLETE message (Figure 5.28).

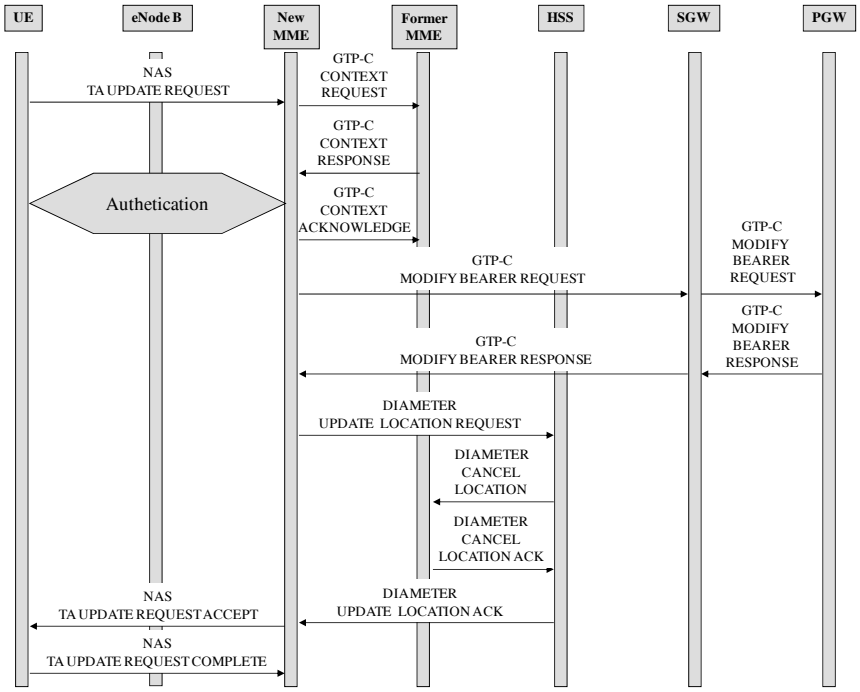


Figure 5.28. *Location updating*

5.3.3. *The establishment of a session*

The establishment of a session is accomplished via several procedures:

– the service request procedure, which is used by the mobile in the idle state or by the PGW entity in order to request the activation of a radio bearer, followed by restarting a session or activating a new service;

– the activation of a new bearer, which corresponds to the activation of a new service when the mobile is in the connected state;

– the modification of an existing bearer, which allows the mobile to modify the bearer characteristics.

5.3.3.1. *Service request*

When the mobile exits the idle state, the radio bearer must be reactivated. The default bearer on the S1-U and S5 interface must be updated. The contexts, however, are maintained in the SGW and PGW entities.

In the case of an outgoing call, the mobile starts the procedure by sending a NAS SERVICE REQUEST message encapsulated in a RRC CONNEXION REQUEST message after the random access procedure. This message is encapsulated by a S1-AP INITIAL UE message in the S1-MME interface. The procedure is followed by activation of the RRC connection (Figure 5.29).

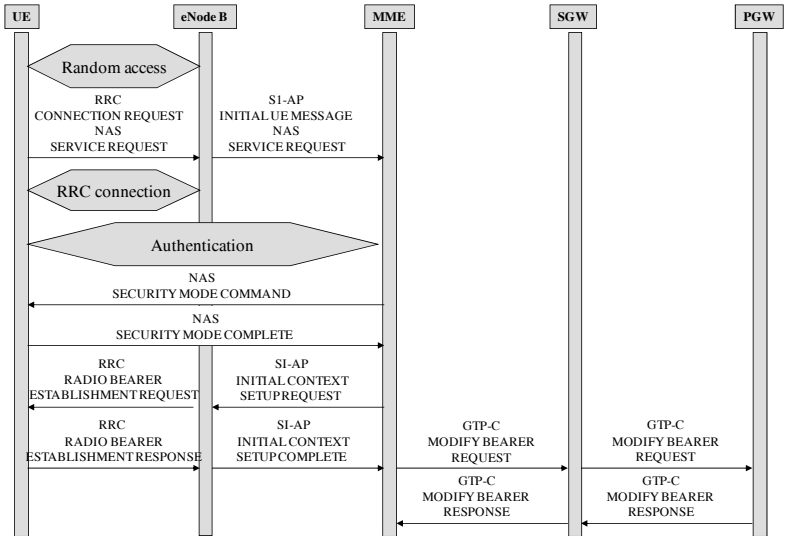


Figure 5.29. *The service request initialized by the mobile*

After the authentication phase, the MME activates the security mechanisms associated with the NAS signaling by exchanging NAS SECURITY MODE COMMAND and SECURITY MODE COMPLETE messages (Figure 5.29).

The MME carries out the same operation regarding the eNode B entity by exchanging S1-AP INITIAL CONTEXT SETUP REQUEST and INITIAL CONTEXT SETUP COMPLETE messages. These allow the eNode B entity to recover the K_{eNB} (Figure 5.29).

The eNode B entity establishes the radio resource via the exchange of RRC RADIO BEARER ESTABLISHMENT REQUEST and RADIO BEARER ESTABLISHMENT RESPONSE signaling (Figure 5.29).

The modification of the bearer on the S1-U and S5 interfaces is activated by the MME and SGW entities via the GTP-C MODIFY BEARER REQUEST and MODIFY BEARER RESPONSE messages respectively (Figure 5.29).

In the case of an incoming call, the SGW entity receives data from the PGW entity while the mobile's traffic plane is not activated. The SGW entity generates the GTP-C DOWNLINK DATA NOTIFICATION message, which is sent to the MME (Figure 5.30).

The MME starts the paging procedure by sending a NAS PAGING message. Upon receiving this message, the mobile initializes the service request procedure (Figure 5.30).

When the different bearers are activated, the SGW entity transfers the incoming data to the eNode B entity, which in turn transmits them to the mobile (Figure 5.30).

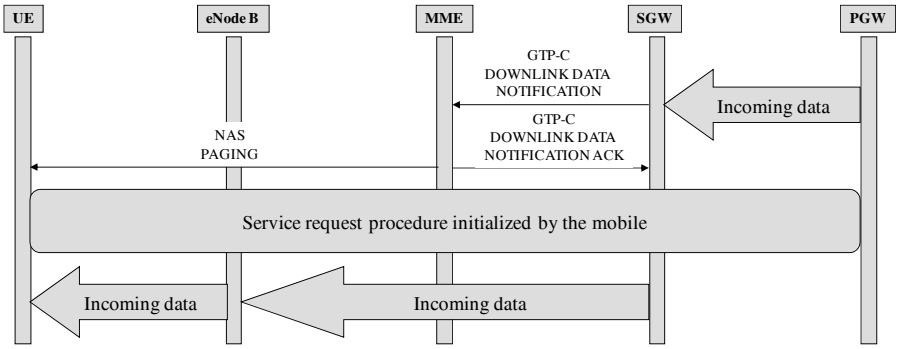


Figure 5.30. *The service request initialized by the SGW entity*

5.3.3.2. *The activation of a new bearer*

The activation of a new bearer, when the mobile is connected, does not need a random access attempt or the establishment of an RRC connection. The PGW entity,

which integrates the PCEF, can initialize the creation of a new bearer, which is triggered by the PCRF.

The request for the creation of the new bearer follows the following stages (Figure 5.31):

– the PGW entity transmits the GTP-C CREATE BEARER REQUEST message to the SGW entity;

– the SGW entity transmits the GTP-C CREATE BEARER REQUEST message to the MME;

– the MME transmits the S1-AP BEARER SETUP REQUEST message to the eNode B entity, encapsulating the NAS SESSION MANAGEMENT REQUEST message;

– the eNode B entity transmits the RRC CONNECTION RECONFIGURATION message to the mobile, encapsulating the NAS SESSION MANAGEMENT REQUEST message.

The different entities successively respond with the following messages (Figure 5.31):

– RRC CONNECTION RECONFIGURATION COMPLETE from the mobile. The bearer is thus created on the radio interface;

– S1-AP BEARER SETUP RESPONSE from the eNode B entity;

– NAS SESSION MANAGEMENT RESPONSE from the mobile;

– GTP-C CREATE BEARER RESPONSE from the MME. The bearer is created on the S1-U interface;

– GTP-C CREATE BEARER RESPONSE from the SGW entity. The bearer is created on the S5 interface.

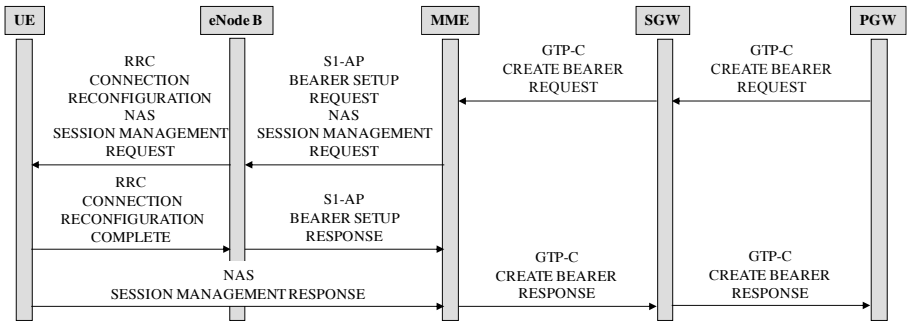


Figure 5.31. *The activation of a new bearer*

5.3.3.3. *The modification of an existing bearer*

The mobile carries out the bearer modification request by sending the NAS REQUEST BEARER RESOURCE MODIFICATION message to the MME (Figure 5.32).

First the MME, then the SGW entity, transmit the GTP-C BEARER RESOURCE COMMAND message (Figure 5.32).

The PECF integrated in the PGW entity checks with the PCRF in order to validate the mobile's request.

If the response is positive, the operations that follow resemble the procedure deployed for the activation of a new bearer.

The bearer modification request follows the following stages (Figure 5.32):

– the PGW entity transmits the GTP-C UPDATE BEARER REQUEST message to the SGW entity;

– the SGW entity transmits the GTP-C UPDATE BEARER REQUEST message to the MME;

– the MME transmits the S1-AP BEARER MODIFY REQUEST message to the eNode B entity, encapsulating the NAS SESSION MANAGEMENT REQUEST message;

– the eNode B entity transmits the RRC CONNECTION RECONFIGURATION message to the mobile, encapsulating the NAS SESSION MANAGEMENT REQUEST message.

The different entities respond successively with the following messages (Figure 5.32):

– RRC CONNECTION RECONFIGURATION COMPLETE from the mobile. The bearer is thus modified on the radio interface;

– S1-AP BEARER MODIFY RESPONSE from the eNode B entity;

– NAS SESSION MANAGEMENT RESPONSE from the mobile;

– GTP-C MODIFY BEARER RESPONSE from the MME. The bearer is modified on the S1-U interface;

– GTP-C MODIFY BEARER RESPONSE from the SGW entity. The bearer is modified on the S5 interface.

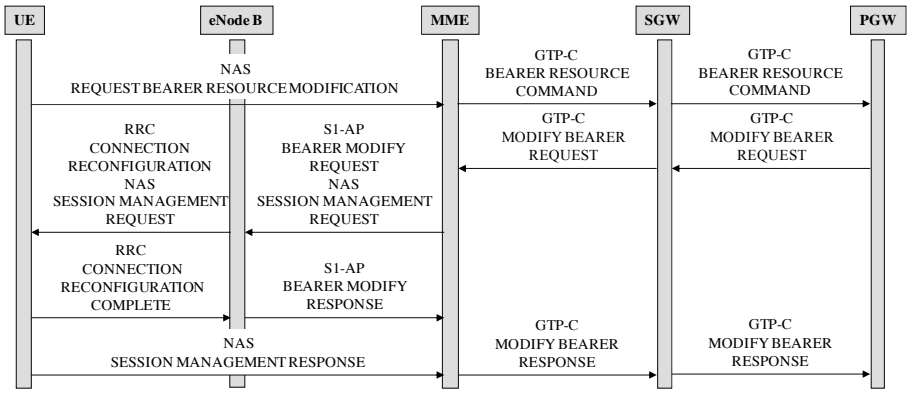


Figure 5.32. *The modification of an existing bearer*

5.3.4. *Mobility procedure*

The handover procedure has two phases:

– the preparation phase, corresponding to the decision to change cell and the reservation of resources;

– the execution phase corresponding to the change of cell, synchronization of the mobile on the target eNode B entity and the release of previous resources.

The various scenarios described depend on the entities intervening in the implementation of the handover.

5.3.4.1. *The intra-eUTRAN handover based on the X2 interface*

This scenario refers to the availability of the X2 interface between two eNode B entities: the source and the target. Two procedures are possible according to whether or not the SGW entity needs to be relocated. Only the procedure without relocation is described.

When the source eNode B entity decides to change cell, it transmits the X2-AP HANDOVER REQUEST message to the target eNode B entity (Figure 5.33).

When the target eNode B entity has allocated the resources, it responds with the X2-AP HANDOVER REQUEST ACK message, encapsulating the HANDOVER COMMAND message that the source eNode B entity will transfer to the mobile (Figure 5.33).

The source eNode B entity also transmits the incoming data that have not been acknowledged by the mobile to the target entity. The target entity will store the data until the mobile is fit to receive them (Figure 5.33).

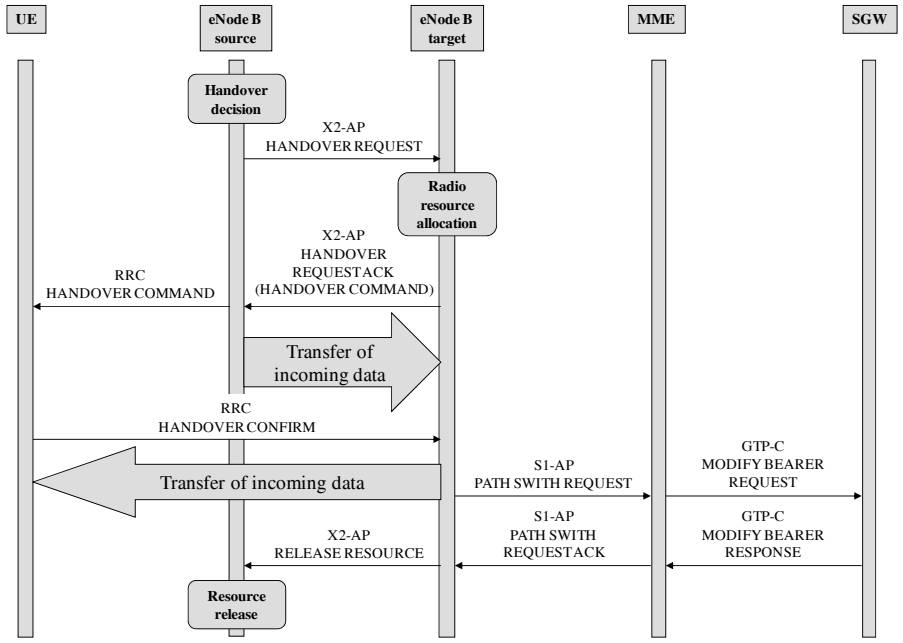


Figure 5.33. *The intra-eUTRAN handover based on the X2 interface, without relocation*

When the mobile is synchronized on the target eNode B entity, it transmits a RRC HANDOVER CONFIRM message. This will trigger the transfer of incoming data and setting-up of the resource on the S1-U interface, via the exchange of following messages (Figure 5.33):

– S1-AP PATH SWITH REQUEST to the MME;

– GTP-C MODIFY BEARER REQUEST to the SGW entity.

When the resource on the S1-U interface is available, the target eNode B entity alerts the source entity in order for it to release the previous resources (Figure 5.33).

5.3.4.2. *The intra-eUTRAN handover based on the S1 interface*

The handover based on the S1 interface occurs when the X2 interface is unavailable. As in the previous case, two procedures are possible depending on whether or not the SGW entity needs to relocate. Only the procedure without relocation is described.

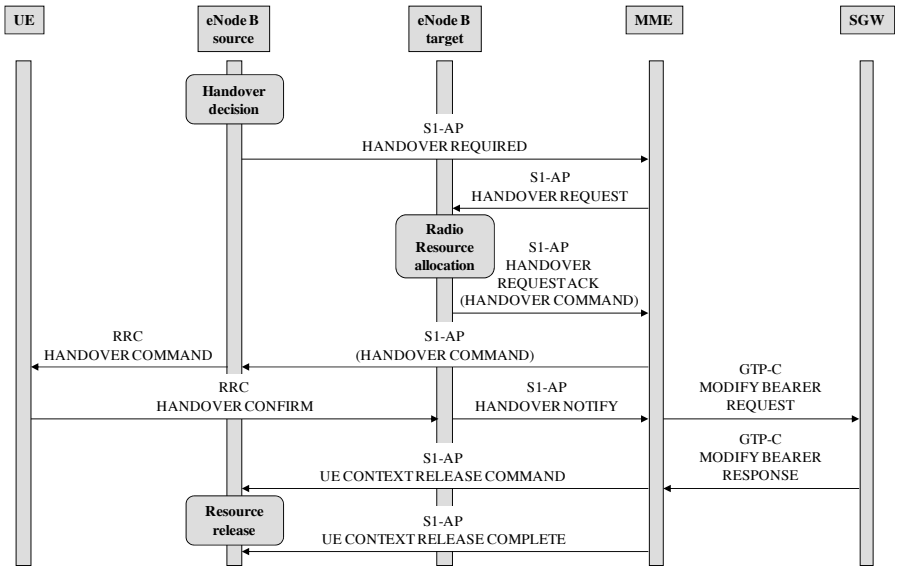


Figure 5.34. *The intra-eUTRAN handover based on the S1 interface, without relocation*

The MME is no longer transparent to the handover mechanism and acts as a signaling relay for the handover command between the source and target eNode B entities (Figure 5.34):

– upon receiving the S1-AP HANDOVER REQUIRED message from the source eNode B entity, the MME generates the S1-AP HANDOVER REQUEST message to be sent to the target eNode B entity;

– upon receiving the S1-AP HANDOVER REQUEST ACK message from the target eNode B entity, the MME transfers the handover command to the source eNode B entity.

Similarly, on the basis of receiving the signaling message confirming the execution of the change of cell, the MME activates the resource on the S1-U interface and provokes release of the radio resource from the source eNode B entity (Figure 5.34)

In addition to this, the incoming data stored at source eNode B entity level, unacknowledged by the mobile, are lost. When the IP header encapsulates a TCP segment that performs a restart in case of an error, the impact results in a decrease in rate. When the IP header encapsulates a UDP segment, such as voice transport on the IP for example, a deterioration in vocal quality occurs.

5.3.4.3. *The inter-system handover*

The inter-system handover is triggered during a change of cell provoking a change in mobile network. Given the coverage level of different technologies, the inter-system handover occurs from the EPS network to the GPRS or UMTS networks, although the inverse is possible.

The inter-system handover is carried out in PS mode. The SGW entity acts as the anchor point and the bearer on the S1-U interface between the eNode B and SGW entities is switched to the S4 interface between the SGSN and SGW entities.

If the SGW entity is not relocated, the PGW entity does not intervene in the handover procedure. However the SGW entity can essentially inform the PGW entity in order to modify the service charges.

The data stored in the eNode B entity, unacknowledged by the mobile, are indirectly transmitted to the SGSN entity via the SGW entity or directly to the RNC entity if there is an interface between the two.

A telephone communication, functioning in PS mode on the EPS network and in circuit service mode on the GSM or UMTS networks, is maintained thanks to the voice call continuity mechanism allowing the transition from PS mode to circuit service mode.

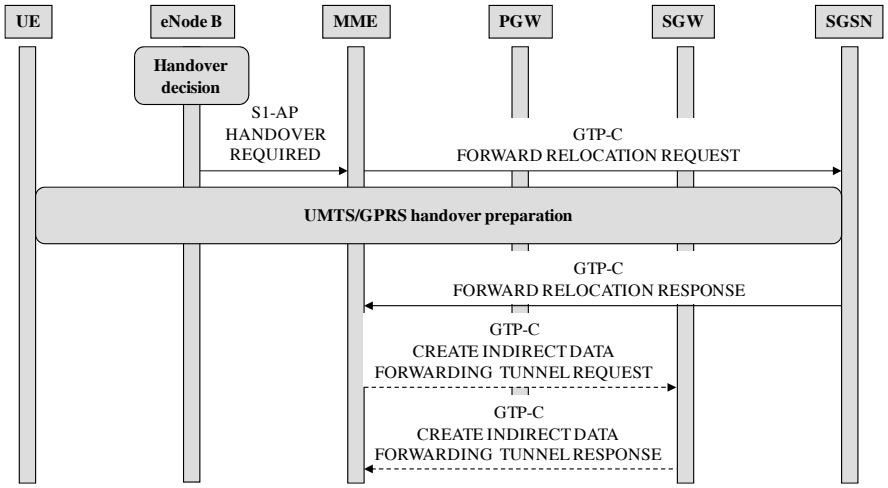


Figure 5.35. *EPS to UMTS inter-system handover – the preparation phase*

The preparation phase is made up of the following messages (Figure 5.35):

– S1-AP HANDOVER REQUEST, which is sent to the MME followed by the decision of the eNode B entity to proceed with the change of cell;

– GTP-C FORWARD RELOCATION REQUEST, which is sent to the SGSN entity.

In the case of an indirect transfer, for which the data between the eNode B and SGSN entities flow via the SGW entity, a signaling exchange is performed between the SGW and SGSN entities by exchanging the GTP-C CREATE INDIRECT DATA FORWARDING TUNNEL REQUEST and RESPONSE messages (Figure 5.35).

Upon receiving the GTP-C FORWARD RELOCATION RESPONSE message, the MME triggers the execution phase by transmitting the S1-AP message to the eNode B entity containing the handover request. The eNode B entity then starts to transfer the stored and unacknowledged data to the SGW entity (Figure 5.36).

When the execution of the handover on the GPRS UMTS networks is terminated, the MME receives the GTP-C FORWARD RELOCATION COMPLETE NOTIFICATION message from the SGSN entity, and triggers the release of the resources (Figure 5.36).

When the data stored have been transferred and the radio resource has been released, the eNode B entity alerts the MME, which in turn releases the bearer on the S1-U interface (Figure 5.36).

The activation of the bearer on the S4 interface is engaged by the SGSN entity, which transmits the GTP-C MODIFY BEARER REQUEST message to the SGW entity.

An update of the context stored in the PGW entity (change of access network) is initialized by the SGW entity via the GTP-C MODIFY BEARER REQUEST message (Figure 5.36).

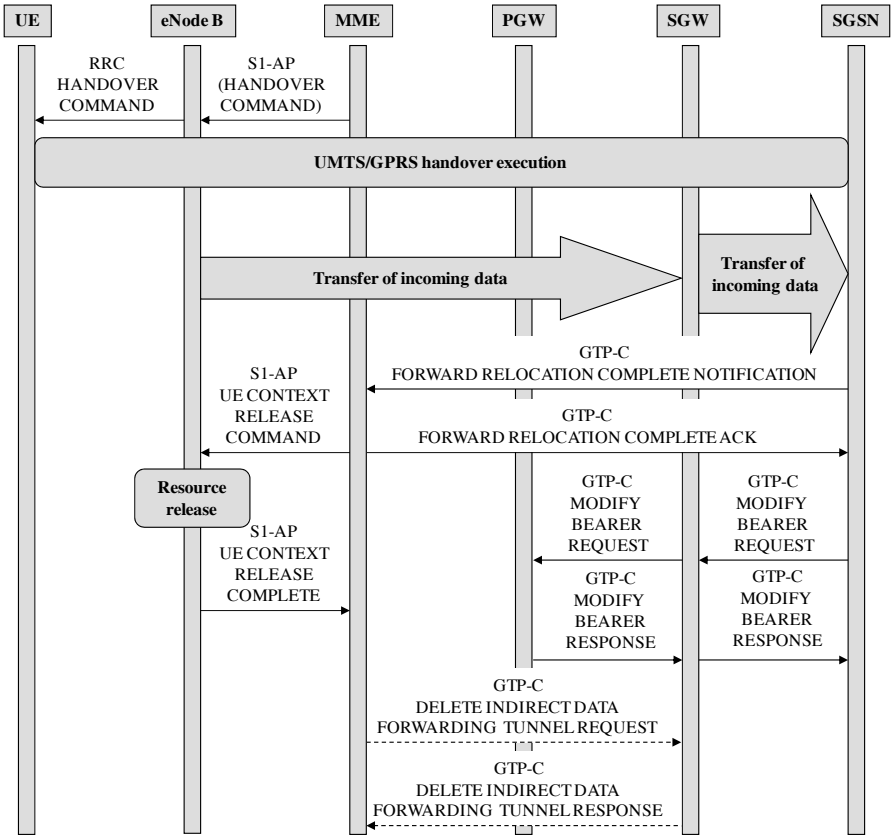


Figure 5.36. *EPS to UMTS inter-system handover – the execution phase*

Chapter 6

The IMS Network

Mobile networks functioning in PS (Packet Service) mode solely carry out the transport of telephone signals (voice and signaling). Signaling processing, which provides the telephone service, is supplied by the IMS (IP Multimedia Subsystem), an entity outside the mobile network.

Section 6.1 explains the SIP (Session Initiation Protocol) that is used to register the user with the telephone service and to establish a session. The SDP (Session Description Protocol) connected to the SIP is used for media negotiation (voice, video and data).

Section 6.2 explains the IMS architecture, which consists of a set of functions in charge of SIP/SDP signaling and media processing. Signaling processing involves the control of the session and the routing of signaling messages. Media flow processing concerns functions that are unavailable in the mobile network, such as the conference and the gateways to the PSTN (Public Switched Telephone Network) fixed telephone networks and the PLMNs (Public Land Mobile Networks).

Section 6.3 describes the procedures concerning the user's registration to the telephone service and the establishment of a session that includes the routing of requests and media negotiation. Media negotiation refers to the control and selection of the media and codec, control of access to the resource and the reservation of resources in the mobile network.

6.1. The SIP

Numerous protocols have been defined to support real-time multimedia data, such as voice, video or text. The SIP functions in conjunction with these protocols by allowing users to mutually discover each other and agree on a description of the session they wish to share.

Details of the session, such as the type of media or codec, are not described by using the SIP. The description of the session is coded in a SDP message connected to the SIP message. The association of both messages fulfills the following functions:

– it determines the location of the extremity that is involved in the communication;

– it establishes the session, including the different phases that concern call processing (numbering, alert, picking-up);

– it determines which media and communication parameters to use;

– it instigates session management, which includes the modification of media during communication and the invocation of services.

6.1.1. *The SIP entities*

The UA (User Agent) is a logical entity located in a telephone terminal (hardphone or softphone), in a gateway or in a telephone application (such as the voicemail inbox).

A UAC (User Agent Client) is the logical entity that creates a request and establishes a transaction. The role of the UAC only lasts for the duration of this transaction. If the UA receives a request later on, it assumes the role of a UAS (User Agent Server) to process this new transaction.

A UAS is the logical entity that generates a response to the received request. The response accepts, rejects or redirects the request. This role only lasts for the duration of this transaction. If the UA later generates a request, it assumes the role of a UAC to process this new transaction.

The registrar is the entity that accepts the REGISTER requests, allowing for registration of the UA. It places the information (the UA's IP (Internet Protocol) address) that it receives in these requests in the Location Service for the domain that it is managing (Figure 6.1).

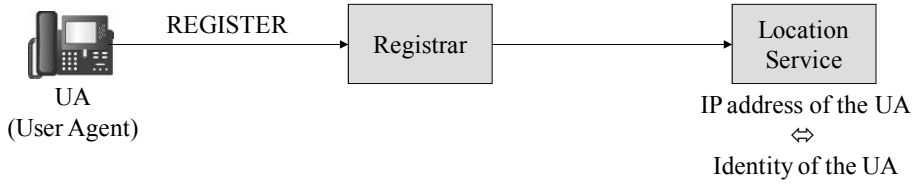


Figure 6.1. *Registration*

The Proxy Server is an intermediary entity that ensures the routing of the INVITE requests, allowing for the establishment of the session as well as the responses. It ensures that the request is sent to another Proxy Server or to the targeted user. A Proxy Server interprets, and if necessary, rewrites specific parts of, a SIP message before its transmission. The Proxy Server can also carry out authentication of the UA that has generated the request (Figure 6.2).

The Redirect Server is a redirection entity which generates a response to the received requests in order to direct the UA to another target.

The Location Service is used by a Proxy Server in order to obtain information regarding the location of the UA that is being called (its IP address).

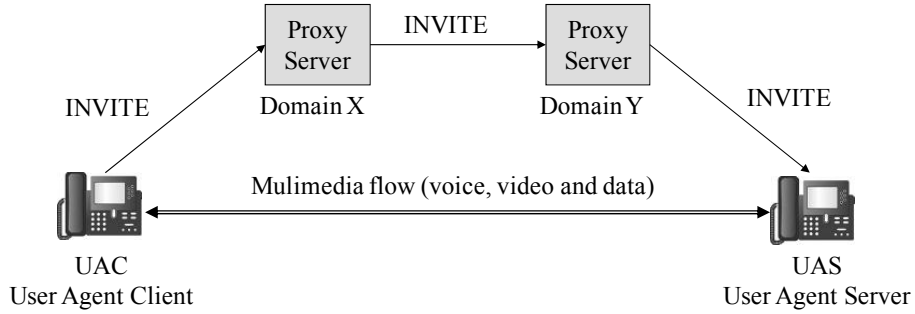


Figure 6.2. *Session establishment*

The B2BUA (Back-to-Back User Agent) is a logical entity that receives a request and treats it as a UAS. In order to determine the response to be conveyed, it acts as a UAC and generates requests to be sent to the target. The B2BUA entity can, for example, be hosted in an Application-Level Gateway in order to translate private addresses into IPv4 public addresses or to translate the IPv4 protocol into the IPv6 protocol.

6.1.2. *The SIP Identity*

A UA has a SIP identity called the SIP URI (Uniform Resource Identifier). Its form is similar to an e-mail address, typically containing the username (for example Alice or Bob) and a domain name (for example a.com or b.com). The two following URIs are thus obtained:

sip:alice@a.com and sip:bob@b.com

SIP also provides a secured URI identity called SIPS URI (for example sips:alice@a.com). The TLS (Transport Layer Security) protocol is used to transport all SIP messages from the caller to the Proxy Server of the person being called. The request is then sent to the person being called, according to the security mechanisms defined in the domain of the person being called.

6.1.3. *The procedures*

Alice's UA uses a SIP application on its softphone or its hardphone to call Bob. Two Proxy Servers, each server acting in their respective domains, facilitate the establishment of a session.

The SIP is based on a pair of HTTP (Hypertext Transfer Protocol) request/responses. Each transaction consists of a request, which involves a particular method, and in one or more responses. Session establishment starts via an INVITE request addressed to Bob's SIP URI. The INVITE request contains a certain number of header fields which contain attributes that provide additional information about a message.

```
INVITE sip:bob@b.com SIP/2.0
Via: SIP/2.0/UDP 20.20.20.20;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@b.com>
From: Alice <sip:alice@a.com>;tag=1928301774
Call-ID: a84b4c76e66710@20.20.20.20
CSeq: 314159 INVITE
Contact: <sip:alice@20.20.20.20>
Content-Type: application/sdp
Content-Length: 142
```

The "Via" header contains the IP address (20.20.20.20) at which Alice waits to receive responses to this request. It also contains a parameter (branch) that identifies this transaction.

The “To” header contains a display name (Bob) and a SIP URI (sip:bob@b.com) or a SIPS URI of where the request was directed.

The “From” header also contains a display name (Alice) and a SIP URI (sip:alice@a.com) or a SIPS URI that indicates the origin of the request. This header field also has a tag parameter that contains a random chain (1928301774) which has been added.

The “Call-ID” header contains a globally unique identifier for the session that is generated by the combination of a random string and an IP address. The combination of the tag of the “To” header and the tag of the “From” and “Call-ID” headers defines the dialog between Alice and Bob.

The “CSeq” header contains an integer and a method name. The CSeq number is incremented for each new request in a dialog.

The “Contact” header contains the SIP URI or the SIPS URI, where the domain name is replaced by the IP address. The “Via” header field indicates where to send the response. The “Contact:” header field indicates where to send the next requests.

The “Max-Forwards:” header is used to limit the number of hops that a request can make on the way to its destination. It consists of an integer that is decremented by one unit at each hop.

The “Content-Type:” header contains a description of the message body (for example SDP).

The “Content-Length:” header indicates the size of the message body.

As Alice’s UA does not know Bob’s IP address, it sends the INVITE request to its Proxy Server, which manages the a.com domain. The IP address of the Proxy Server can be configured manually or dynamically (for example via the DHCP (Dynamic Host Configuration Protocol)) in Alice’s UA (Figure 6.3).

The Proxy Server receives the INVITE request and sends a 100 Trying response to Alice’s UA. The 100 Trying response indicates that the INVITE request has been received and that the Proxy Server will deal with it in order to ensure its delivery to the target (Figure 6.3).

The responses in SIP use a three-figure code followed by a descriptive phrase. This response contains the same headers “To”, “From”, “Call-ID”, “CSeq” and the branch parameter in the “Via” header of the INVITE request, which allows Alice’s UA to correlate this response with the transmitted request (Figure 6.3).

Proxy Server a.com locates Proxy Server b.com by carrying out a DNS (Domain Name Service) resolution. Consequently, it obtains Proxy Server b.com's IP address (Figure 6.3).

Before transferring the request, Proxy Server a.com adds a new "Via" header containing its own address. Note that the INVITE request already contains Alice's address in the first "Via".

Proxy Server b.com receives the INVITE request and responds to Proxy Server a.com with a 100 Trying in order to indicate that the INVITE request has been received and that the Proxy Server is processing it to ensure its delivery to the target (Figure 6.3).

Proxy Server b.com consults the Location Service that contains Bob's IP address. It adds a new "Via" header containing its own address and transfers the INVITE request to Bob's UA (Figure 6.3).

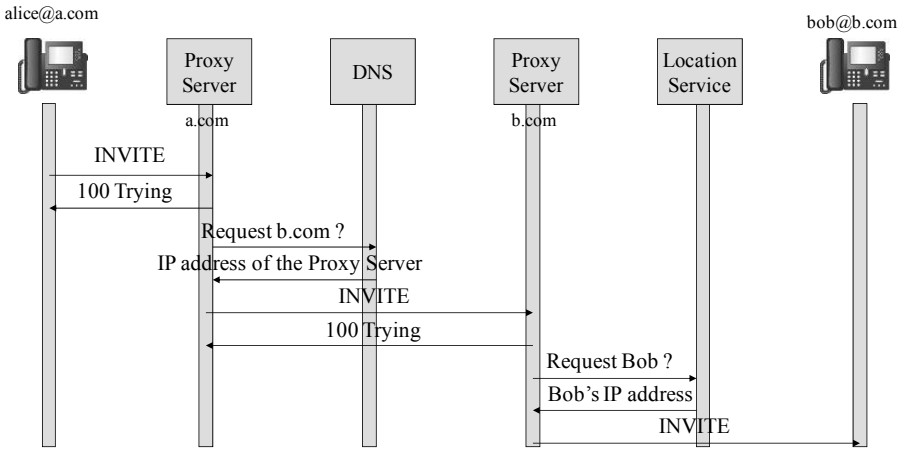


Figure 6.3. *Routing of the INVITE request*

Bob's UA receives the INVITE request and an alert is used to inform Bob of an incoming call. Bob's UA sends a 180 Ringing response. Each Proxy Server uses the "Via" header to determine where to send the response, and removes the "Via" header that contains its own address (Figure 6.4).

When Alice's UA receives the 180 Ringing response, Alice is given a ringback tone.

When Bob picks up his handset, it sends a 200 OK response. The 200 OK response contains a SDP message body that contains the description of the type of session that Bob is ready to establish with Alice (Figure 6.4).

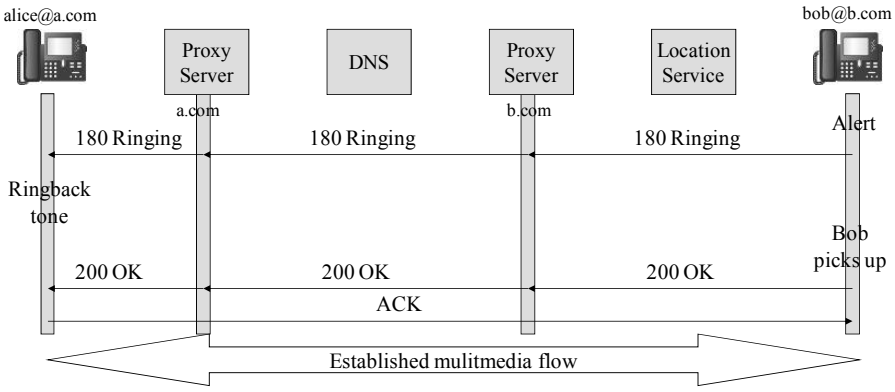


Figure 6.4. *Routing of the responses*

Consequently, there is a two-phase exchange of SDP messages. Alice has sent a (offer) SDP message in the INVITE request to Bob. In return, Bob has sent a (response) SDP message to Alice.

The different types of responses are clarified in Table 6.1.

Type of response	Designation
1xx	Temporary response
2xx	Definitive and positive response
3xx	Definitive redirection response
4xx	Definitive and negative response – client failure
5xx	Definitive negative response – network failure
6xx	Definitive and negative response – global failure

Table 6.1. *The types of SIP responses*

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP server.b.com;branch=z9hG4bKnashds8
Via: SIP/2.0/UDP server.a.com;branch=z9hG4bK77ef4c
Via: SIP/2.0/UDP 20.20.20.10;branch=z9hG4bK776asdhds
To: Bob <sip:bob@b.com>;tag=a6c85cf
From: Alice <sip:alice@a.com>;tag=1928301774
Call-ID: a84b4c76e66710@20.20.20.20.com
CSeq: 314159 INVITE
Contact: <sip:bob@30.30.30.30>
Content-Type: application/sdp
Content-Length: 131
```

The first line of the response contains the response code (200) and the reason phrase (OK). The remaining lines contain the headers.

The headers “Via”, “To”, “From”, “Call-ID” and “CSeq” are copied from the INVITE request. There are three “Via” headers: the first was added by Alice’s UA, the second by Proxy Server a.com, and the third by Proxy Server b.com.

Bob’s UA added a tag parameter to the “To” header, which is used to complete the identification of the dialog initialized with the ‘Call-ID’ header and the tag field of the ‘From’ header.

The “Contact” header contains a URI where Bob can be reached directly on his SIP telephone.

The “Content-Type” header contains a description of the message body (for example SDP).

The “Content-Length” header indicates the size of the message body.

The 200 OK response is relayed by both Proxy Servers and is received by Alice’s UA, which stops the ringback tone.

Alice’s UA sends an ACK acknowledgment message to Bob’s UA in order to confirm that is has received the 200 OK response. In this example, the acknowledgment is sent directly, without flowing via the Proxy Servers. This is possible because Alice has recovered Bob’s IP address from the “Contact” header of the “200 OK” response.

Alice and Bob’s UAs start the session and exchange data by using the format agreed during the exchange of SDP messages.

During the session, Alice or Bob can decide to modify the characteristics of the media, for example transition from a telephone session to a videophone session. This is done by sending a new INVITE (re-INVITE) request containing the description of the new media. This new request contains the same dialog identifiers so that the other part knows that the request is about a modification of the existing session.

The other part sends a 200 OK response in order to accept the change. The part that is calling responds to the 200 OK with an ACK acknowledgement. If the other part does not accept the change, it sends a 488 Not Acceptable response, and the one that is calling also sends an acknowledgement. The failure of the INVITE request does not cause the current call to cut-off, however. The session continues to use the previously-negotiated characteristics.

At the end of the call, Bob hangs up first and a BYE message is sent directly to Alice's UA without flowing via the Proxy Servers. Alice confirms receipt of the BYE request with a 200 OK, which terminates the dialog (Figure 6.5).

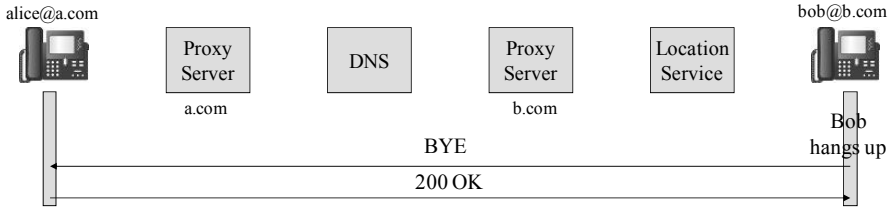


Figure 6.5. *Routing of subsequent requests without relaying the Proxy Servers*

In some cases, it can be useful when Proxy Servers can see all subsequent requests exchanged between Alice and Bob's UAs (ACK, re-INVITE, BYE). For this, the Proxy Servers add a "Record-Route" header that contains the IP address of the Proxy Server to the INVITE request. This information is received by Bob's UA in the INVITE request, and by Alice's UA in the 200 OK response (Figure 6.6).

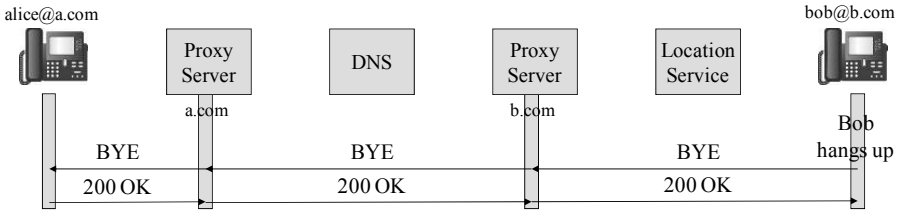


Figure 6.6. *Routing of the subsequent requests with relaying of the Proxy Servers*

6.2. The IMS architecture

The IMS network provides the multimedia services (telephony, videotelephony and data) when the mobile network uses the PS mode. It connects to the GGSN (Gateway GPRS Support Node) of the UMTS (Universal Mobile Telecommunications System) network or to the PDN GW (Packet Data Network GateWay) of the EPS (Evolved Packet System) network (Figure 6.7).

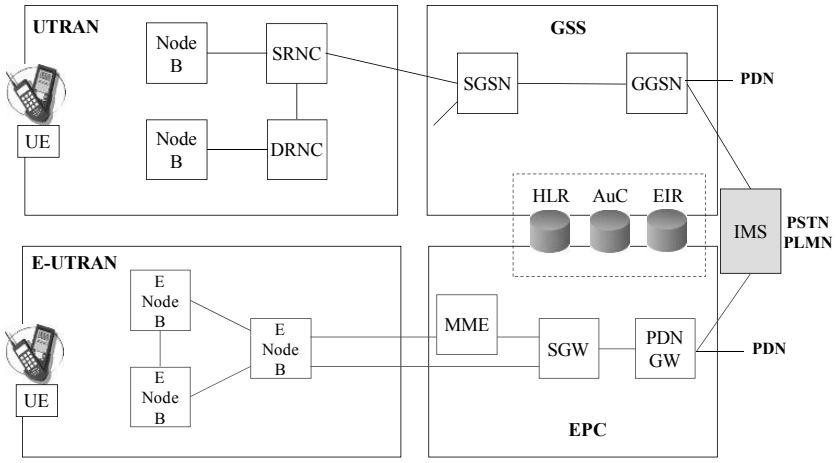


Figure 6.7. *The positioning of the IMS network*

The IMS network includes the following entities (Figure 6.8):

– the control of CSCF (Call Session Control Function) sessions, which include the P (Proxy)-CSCF, S (Serving)-CSCF, I (Interrogating)-CSCF and E (Emergency)-CSCF functions;

– the application servers containing the AS (Application Server) function;

– the databases containing the SLF (Subscription Locator Functional) and HSS (Home Subscriber Server) functions;

– MRF (Multimedia Resource Function) multimedia flow processing containing the MRFC (MRF Controller) and MFRP (MFR Processing) functions;

– the interconnection with the PSTN fixed telephone networks or with the PLMN s containing the BGCF (Breakout Gateway Control Function), MGCF (Media Gateway Control Function), MGW (Multimedia GateWay) and SGW (Signaling Gateway) functions. The MGCF, MGW and SGW functions are identical to those described for the Next Generation Network;

– offline and online charging.

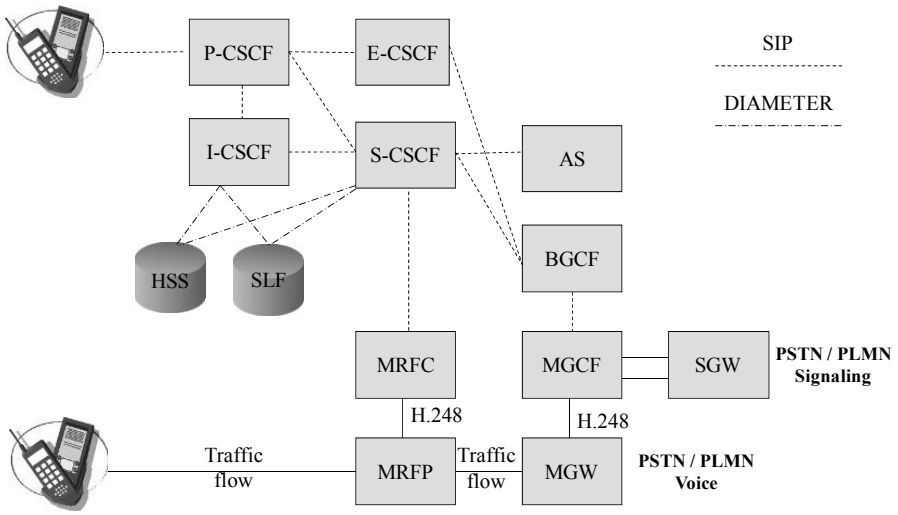


Figure 6.8. *The IMS network entities*

6.2.1. *Control of sessions*

6.2.1.1. *The P-CSCF*

The P-CSCF is the first point of contact for the UE (User Equipment) of the IMS network. It ensures the function of the Proxy Server. It receives requests from the UE or S-CSCF and transfers them to the S/I-CSCF or to the UE, respectively. The P-CSCF does not modify the URI request of the SIP INVITE message. It can also act as a UA in abnormal functioning conditions, when it must terminate or generate SIP transactions.

The tasks performed by the P-CSCF are as follows:

– it transfers the SIP REGISTER request to the I-CSCF function determined from the domain name provided by the UE. It adds a Path header containing its IP address to the message;

– it transfers the SIP INVITE request received from the S-CSCF (or the UE, respectively) to the UE (or the S-CSCF, respectively). In order to carry out the transfer, the P-CSCF function must recover the IP addresses from the UE (S-CSCF, respectively). The SIP INVITE request received from the S-CSCF contains the UE's IP address instead of the URI. The SIP INVITE request received from the UE contains the IP address of the S-CSCF in the Route header;

– it detects emergency calls and transfers them to the E-CSCF function;

– it generates the information necessary for the generation of the charging tickets;

– it establishes an IPSec security association with the UE during its registration;

– it controls the type of resources required by the UE according to the capabilities offered by the mobile network;

– it verifies the availability of resource in the mobile network.

6.2.1.2. *The I-CSCF*

The I-CSCF (Interrogating CSCF) is the point of contact with the interior of the IMS network for certain transactions from the P-CSCF located either in the host mobile network or in the mobile network that is visited. It ensures the function of the Proxy Server.

The tasks performed by the I-CSCF are as follows:

– upon receiving the first SIP REGISTER request, it assigns a S-CSCF to the UE and transfers the request to the S-CSCF. In order to carry out this function, an exchange of messages with the HSS is necessary;

– upon receiving the second SIP REGISTER request and the first SIP INVITE request for an incoming call, it queries the HSS in order determine the S (Serving)-CSCF allocated to the UE and transfers the request to it;

– it generates the information necessary for the generation of charging tickets.

6.2.1.3. *The S-CSCF*

The S-CSCF provides the session control services to the UE. It ensures different roles according to the type of request received:

– for registration of the UE, it ensures the Registrar function;

– for the establishment of a session, it ensures the Proxy Server function;

– in abnormal functioning conditions, when it must terminate or generate SIP transactions, it can also act as a UA.

The tasks performed as Registrar are as follows:

– upon receiving the first REGISTER request, the Registrar contacts the HSS in order to recover the UE's authentication data. It responds with a 401 message containing the parameters used for authentication;

– upon receiving the second REGISTER request, the Registrar authenticates the UE and recovers its profile from the HSS. It responds with a 200 OK message containing a Service Route header with its IP address.

The tasks performed by Proxy Server are as follows:

– for an outgoing call, upon receiving the first SIP INVITE request from the P-CSCF, the Proxy Server carries out a control on the requested service. It transfers the request to the AS or to the I-CSCF belonging to the mobile network of the requested UE, or it transfers the request to the BGCF if the requested UE is not in an IMS network. The IP address of the AS is contained in the UE profile recovered during registration;

– for an incoming call, upon receiving the first SIP INVITE request from the I-CSCF, the Proxy Server carries out a control on the requested service. It either transfers the request to the AS or to the P-CSCF. In the latter case, it replaces the URI of the request with the IP address of the UE. The IP address of the P-CSCF is recovered from the Path header, during the registration of the UE;

– the Proxy Server generates the information necessary for the generation of charging tickets.

6.2.1.4. *The E-CSCF*

The E-CSCF processes emergency calls transmitted by the P-CSCF and routes the request to the PSAP (Public Safety Answering Point) emergency center. The PSAP can be connected to a mobile, a fixed telephone network or to an IMS network.

The tasks performed by the E-CSCF are as follows:

– upon receiving the SIP INVITE request, the E-CSCF contacts the LRF (Location Retrieval Function) in order to obtain the UE's location or to confirm whether it is included in the request;

– on the basis of information also supplied by the LRF, it transfers the request to the PSAP emergency center.

6.2.2. *The Application Servers*

The AS (Application Server) function provides value-added services to the IMS network. It hosts and executes services. It can impact the SIP session based on the service required. It can be located in the host network or be provided by a third party.

The S-CSCF must decide whether an AS is necessary in order to receive information concerning a SIP request so as to ensure the appropriate service is processed. The decision is based on the information received from the HSS function during user registration.

The application server can serve many roles in the processing of a SIP message:

– that of a Proxy Server: in this mode, the SIP request from the S-CSCF is sent back to the S-CSCF. The application server can add, remove or modify the headers of the SIP message;

– that of a UAS or a Redirect Server: in this mode, the application server's response to the SIP request from the S-CSCF is of the type 2xx, 4xx, 5xx, 6xx (for UASs) or 3xx (for Redirect Servers);

– that of UAC: in this mode, the application server generates the SIP request and transmits it to the S-CSCF;

– that of a B3BUA: in this mode, the application server receiving a SIP request from the S-CSCF terminates the dialog and generates a new request.

6.2.3. *The databases*

The HSS function is a database that ensures the storage of each user's data. The main stored data include user identities, access parameters and service release information.

The user identities include the public and private identities. The private identity is an identity allocated by the IMS network operator. It is used for registration. The public identity is the identity that other users can use to establish a session. The access parameters are used for authentication of the user during registration. The service release information is used by the S-CSCF to transfer a SIP request to an application server.

The SLF allows CSCFs to find the address of the HSS, which contains the subscriber data when several devices containing the HSS function are deployed in the IMS network.

6.2.4. *The interconnection*

The BGCF deals with the routing requests transmitted by the S-CSCF when the session cannot be delivered in the IMS network. This concerns the calls to users connected to a PSTN or PLMN.

The BGCF determines the next hop in the SIP message delivery. It must choose the MGCF responsible for interworking with the PSTN or PLMN. If the interconnection function is located in the other network, it transmits the SIP message to another BGCF located in the selected network.

6.2.5. *Multimedia flow processing*

The MRF entity is divided into two functions: MRFC and MRFP (MRF Processor).

The tasks performed by the MRFC are as follows:

– it controls the media resources of the MRFP function;

– it interprets information from the S-CSCF and consequently controls the MRFP function;

– it generates the information necessary for the generation of charging tickets.

The tasks performed by the MRFP are as follows:

– it generates media flows under the control of the MRFC function (e.g. telephone listings);

– it mixes the media flows in order to provide a conference service;

– it ensures media flow processing, such as transcoding of the audio signal.

6.2.6. *Charging*

In order to feed the tariff mechanisms, the IMS network monitors the use of resources in real-time in order to detect the events relevant for charging.

In the case of offline charging, the use of the resources is signaled after the resources are used. This case corresponds to a subscription service. In the case of online charging, the user's account is queried before getting permission to use the network resource. This case corresponds to a prepaid service.

6.2.6.1. *Offline charging*

Offline charging is a process where the charge information for the use of network resources is collected at the same time as the resources are being used.

The CTF (Charging Trigger Function) generates charge events based on observation of the use of network resources. It is integrated into all of the IMS network functions (Figure 6.9).

The CDF (Charging Data Function) receives the charge information from the CTF. It then uses the information to construct CDR (Charging Data Record) tickets. DIAMETER is the protocol for the exchange of messages between these two functions (Figure 6.9).

The CDR tickets produced by the CDF are immediately transferred to the CGF (Charging Gateway Function), a database that acts as a gateway with the billing system (Figure 6.9).

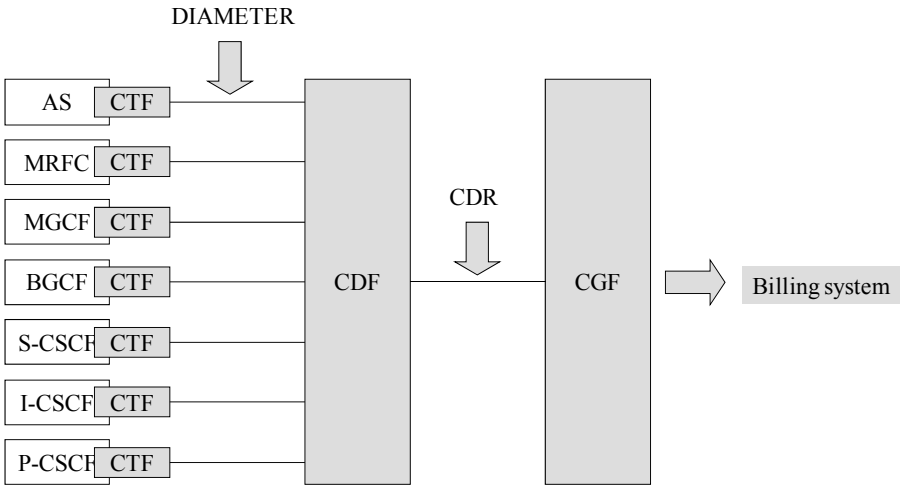


Figure 6.9. *Offline charging*

6.2.6.2. *Online charging*

The S-CSCF does not trigger any charge event and does not include the CTF. The online pricing is transparent for this function and appears as service logic controlled by an IMS-GW (IMS Gateway) application server (Figure 6.10).

The OCS (Online Charging System) function consists of several distinct modules (Figure 6.10):

– charging on the basis of sessions opened by the user (e.g. voice calls);

– charging on the basis of events in conjunction with application servers;

– enhancement of the use of network resources in order to calculate the amount to be charged;

– the balance of the user's account.

The generation of CDR tickets to the billing system is optional. It is implemented by the same entities as in the case of offline charging (Figure 6.10).

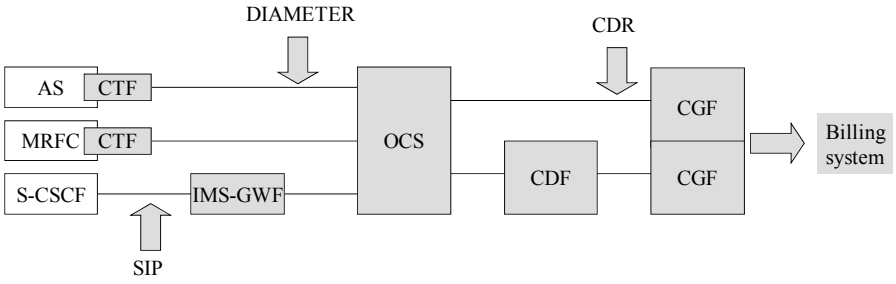


Figure 6.10. *Online charging*

6.3. Communication management

6.3.1. *Registration*

The relevant information required for registration is obtained from the ISIM (IMS Services Identity Module) contained in the UICC (Universal Integrated Circuit Card) of the UE mobile. Registration is carried out in two phases in order to authenticate the mobile. If authentication of the mobile by the UMTS or EPS network can be recovered by the mobile network, the registration is carried out in a single phase.

The first phase of registration has the following stages (Figure 6.11):

– the mobile sends a first REGISTER request containing its private identity to the P-CSCF;

– the P-CSCF transfers the REGISTER message to the I-CSCF by including its IP address in the Path header;

– the I-CSCF contacts the HSS function for selection of the S-CSCF and transmits the REGISTER request to the S-CSCF; and finally

– the S-CSCF function contacts the HSS to recover the authentication data from the mobile and responds to it with a 401 Unauthorized message.

At this stage, the IP address of the S-CSCF is registered in the HSS and that of the P-CSCF in the S-CSCF.

The mobile authentication data consist of a quintuplet:

– a challenge RAND transmitted to the mobile in the 401 Unauthorized message;

– the result expected from the challenge, XRES;

– the authentication token of the network transmitted (AUTN – Authentication of the Network) to the mobile in the 401 Unauthorized message;

– the integrity key (IK) for the establishment of the IPSec security association between the mobile and the P-CSCF;

– the cipher key (CK) for the establishment of the IPSec security association between the mobile and the P-CSCF.

The IK and CK are solely transmitted to the P-CSCF in the 401 Unauthorized message.

Upon receiving the 401 Unauthorized message, the mobile authenticates the IMS network and calculates the RES response to the challenge RAND on the basis of a secret contained in the ISIM. It also calculates the IK integrity and the CK cipher keys.

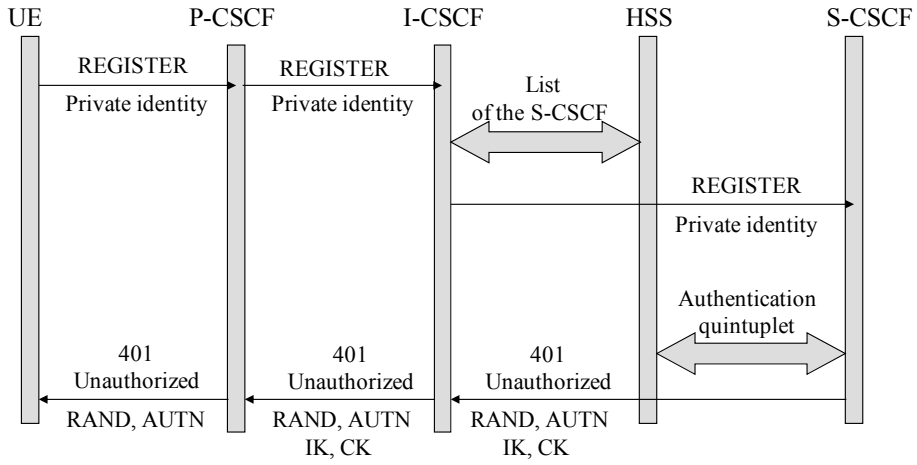


Figure 6.11. *The first phase of registration*

The second phase of registration involves the following stages (Figure 6.12):

– the mobile sends a second REGISTER request containing the private identity and the RES response to the P-CSCF;

– the P-CSCF transfers the REGISTER message to the I-CSCF;

– the I-CSCF contacts the HSS function in order to recover the IP address of the S-CSCF and transmits the REGISTER request to it;

– the S-CSCF function compares the value of the received RES with that of the XRES. If both values are identical, the mobile is authenticated;

– the S-CSCF contacts the HSS in order to recover the mobile's profile and responds to it with a 200 OK message by including its IP address in the Service Route header.

At this stage, the S-CSCF function has created a connection between the public identity of the mobile and its IP address. This is so that it can subsequently route the calls to the mobile. The mobile has recovered the IP address from its S-CSCF.

The registration is effective for a duration specified in the 200 OK response. The mobile must reregister before the end of this time by following the same procedure as the initial registration.

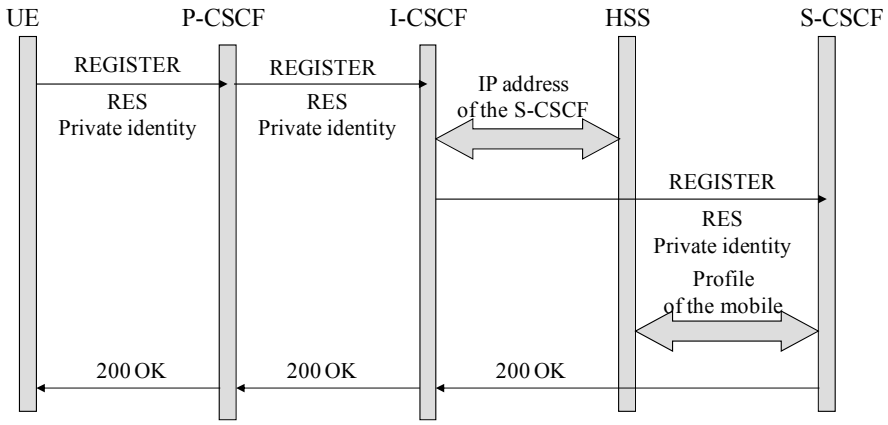


Figure 6.12. *The second phase of registration*

Deregistration can be carried out in different ways:

– by the mobile, when the user switches off their mobile;

– by the P-CSCF, when the mobile is no longer under the radio coverage of the UMTS or EPS network. The PCRF (Policy and Charging Rules Function) communicates this information to the P-CSCF;

– by the S-CSCF, when the user has cancelled their contract.

Deregistration by the mobile uses the REGISTER method by indicating a zero duration. Deregistration via the P-CSCF or S-CSCF uses the NOTIFY method.

6.3.2. *The session*

6.3.2.1. *Routing of requests*

Alice (URI sip: alice@a.com) wishes to establish a communication with Bob (URI sip: bob@b.com). Alice's UE generates an initial INVITE request containing (Figure 6.13):

– Bob's URI in the request;

– the IP address of the S-CSCF of the domain (a.com) contained in the Route header. This address is acquired during the registration of Alice's UE (information contained in the Service Route header).

Alice's UE transmits the INVITE request to the P-CSCF of the domain (a.com). It adds a Record Route header containing its own IP address and transfers the request to the S-CSCF of the domain (a.com) whose IP address is contained in the Route header. The Record Route header is the route used by subsequent requests (Figure 6.13).

The S-CSCF of the domain (a.com) removes the Route header containing its own IP address. It recovers the destination domain name (b.com) from Bob's URI and contacts a DNS (Domain Name Service) server to recover the IP address of the I-CSCF of the domain (b.com). It adds a Record Route header containing its own IP address and transfers the request to the I-CSCF of the domain (b.com), see Figure 6.13.

The I-CSCF of the domain (b.com) contacts the HSS function in order to recover the IP address of S-CSCF of the domain (b.com) having registered Bob's UE. It does not add a Record Route header and transfers the request to the S-CSCF of the domain (b.com), see Figure 6.13.

The S-CSCF of the domain (b.com) modifies the initial request by replacing Bob's URI with its IP address. The connection between the URI and the IP address was created during the registration. It adds a Record Route header containing its

own IP address and transfers the request to the P-CSCF of the domain (b.com). The IP address of the P-CSCF allocated to Bob's UE was learnt during the registration (information contained in the Path header), see Figure 6.13.

The P-CSCF adds a Record Route header containing its own IP address and transfers the request to Bob's UE, whose IP address is included in the request (Figure 6.13).

Bob's UE stores the different Record Route headers that will later be used for routing subsequent requests. It transmits a 183 Session Progress response to Alice's UE containing the received Record Route headers. This will allow Alice to recover the IP addresses of the CSCFs before dealing with the subsequent requests (Figure 6.13).

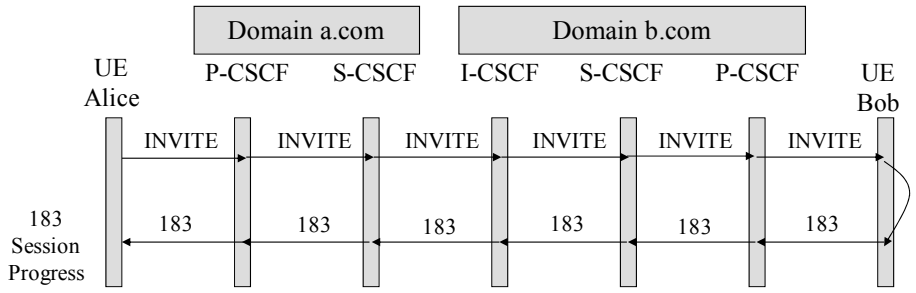


Figure 6.13. *Routing of the initial request*

Alice's UE sends the subsequent PRACK request in order to acknowledge the temporary 183 Session Progress response. It indicates in the Route headers the IP addresses of the functions dealing with the request in order to be able to determine the P/C-CSCFs of the domains (a.com and b.com), see Figure 6.14.

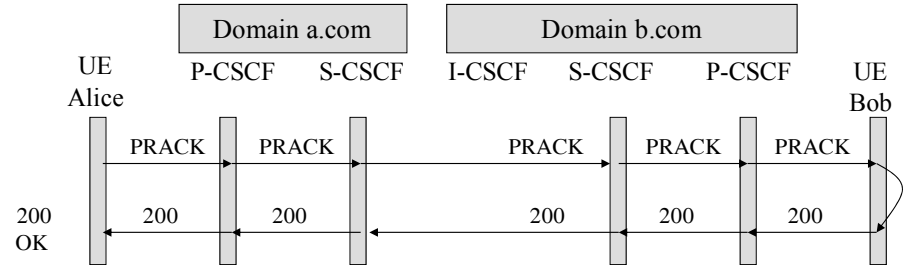


Figure 6.14. *Routing of the subsequent request*

6.3.2.2. *Media negotiation*

6.3.2.2.1 Media control

The P-CSCF can interact with the PCRF in order to obtain the parameters of the media authorized by the mobile network. It examines the information contained in the SDP message carried by the INVITE request. If it finds that these cannot be used by the mobile network, it transmits a negative 488 Not Acceptable Here response to Alice's UE. This rejection must contain sufficient information to allow Alice's UE to initialize a new attempt with the parameters of the authorized media.

During registration, the HSS function supplies the user's profile, containing the parameters of the media authorized by the service provided, to the S-CSCF. Similarly, the S-CSCF examines the information contained in the SDP message carried by the INVITE request. If it finds that these do not conform to the service profile, it transmits a 488 Not Acceptable Here negative response to Alice's UE.

6.3.2.2.2. Media and codec selection

Alice's UE sends a first SDP offer in the initial INVITE request to Bob's UE. The offer lists all media types (audio and video) that Alice wishes to use for this session as well as the list of the different codecs supported (Figure 6.15).

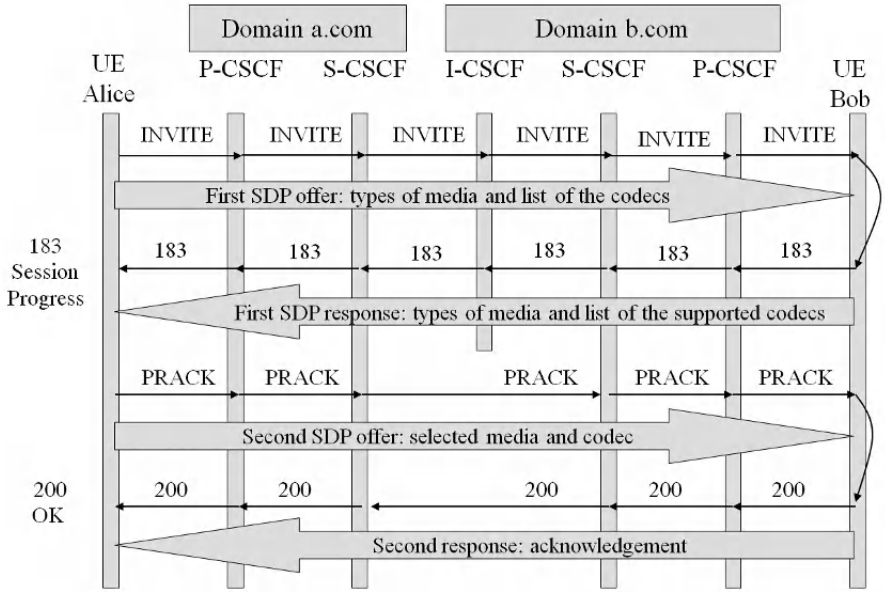


Figure 6.15. *Media and codec selection*

In the 183 Session Progress response, Bob's UE provides a first SDP response in which it can reject certain types of media proposed and reduce the list of codecs in such a way that only the codecs supported by the two extremities are considered (Figure 6.15).

Alice's UE makes the final decision on the codecs used. It sends a second SDP offer to Bob's UE in the subsequent PRACK request, which indicates a unique codec for each type of bearer that will be used during the session (Figure 6.15).

Bob's UE accepts the second offer and sends confirmation in the 200 OK response (Figure 6.15).

6.3.2.2.3. Resource access control

When the P-CSCF of domain b.com receives the INVITE request, it queries the PCRF in order to obtain an authorization token for mobile network resource access. This token is transmitted to Bob's UE in the INVITE request (Figure 6.16).

The PCRF also transfers the token to the PCEF (Policy and Charging Enforcement Function). When Bob's UE initializes the resource reservation, it presents the received token. The resource access is controlled by the PCEF by comparing the tokens received from the PCRF and from Bob's UE (Figure 6.16).

Similarly, when the P-CSCF of domain a.com receives the 183 Session Progress response, it queries the PCRF in order to obtain an authorization token for mobile network resource access. This token is transmitted to Alice's UE in the 183 Session Progress response (Figure 6.16).

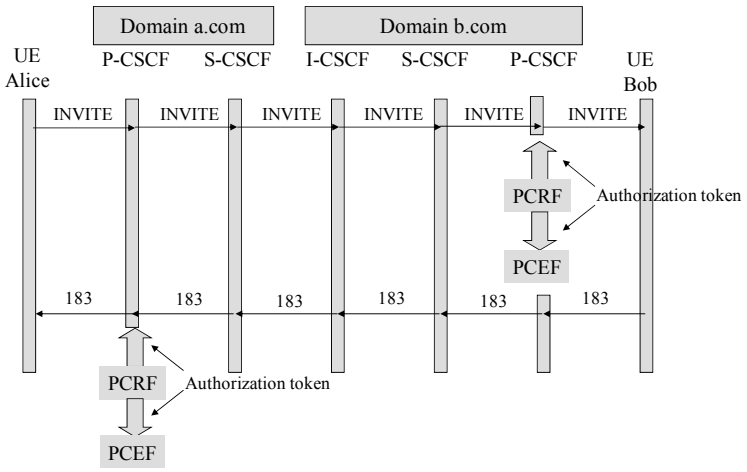


Figure 6.16. *Resource access control*

6.3.2.2.4. Preconditions

When the establishment of the session is conditioned to the establishment of the resource, Alice and Bob's UEs will exchange information regarding preconditions in the media negotiation SDP messages (Figure 6.17):

– Alice's UE indicates in the first SDP offer of the SIP request that it needs to reserve a resource before establishing a session;

– Bob's UE indicates in the first SDP response of the 183 Session Progress response that it also needs to reserve a resource before establishing a session;

– Alice's UE makes the resource reservation on the mobile network and transmits the second SDP offer in the PRACK message;

– Bob's UE carries out resource reservation on the mobile network and transmits the second SDP acknowledgement response contained in the 200 OK response;

– when Alice's UE has confirmation of the resource reservation, it indicates this to Bob's UE in a third SDP offer contained in an UPDATE request;

– when Bob's UE has confirmation of the resource reservation, it indicates this to Alice's UE in the third SDP response contained in the 200 OK request.

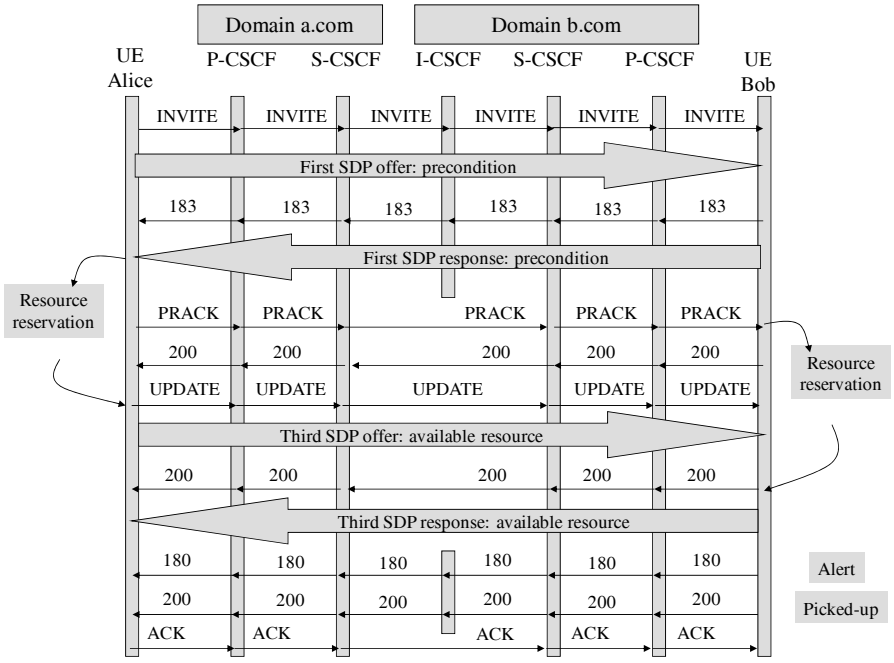


Figure 6.17. *The preconditions*

When the resource reservations are effective at each extremity, Bob's telephone can ring and a 180 Ringing response is transmitted to Alice's UE, generating the ringback tone at its level. When Bob picks up, a 200 OK response is transmitted to Alice's UE, which acknowledges it via the subsequent ACK request. The session is thus established (Figure 6.17).

6.3.2.3. *Termination of the session*

Termination of the session can be triggered by the UE, the P-CSCF or IMS-GWF (IMS Gateway Function), with the help of the BYE method.

Termination of the session can be initialized by any UE when the communication is terminated (Figure 6.18, case 1).

The P-CSCF can also end the session if the mobile is no longer under radio coverage (Figure 6.18, case 2). The PCRF provides this information to the P-CSCF.

The IMS-GWF terminates the session, if it is prepaid, when the user's credit has been consumed (Figure 6.18, case 3). The OCS function supplies this information to the IMS-GWF. Two BYE requests are necessary to terminate the session: one request to Alice's UE and the second to Bob's UE.

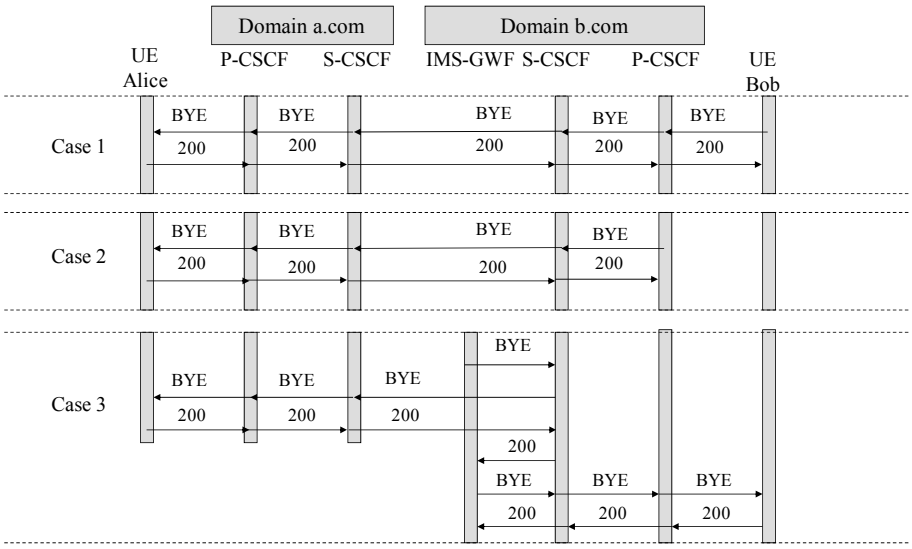


Figure 6.18. *Termination of the session*

List of Abbreviations

A

AAL2	ATM Adaptation Layer
AGCH	Access Grant CHannel
AICH	Acquisition Indicator CHannel
ALG	Application-Level Gateway
AMR	Adaptative MultiRate
AN	Access Network
ANM	ANswer Message
APM	APplication transport Mechanism
APN	Access Point Name
AS	Access Stratum
AS	Application Server
ATM	Asynchronous Transfer Mode
AuC	Authentication Center

B

B2BUA	Back-to-Back User Agent
BCCH	Broadcast Control CHannel
BCH	Broadcast CHannel
BCS	Block Check Sequence
BCTP	Bearer Control Tunneling Protocol
BG	Border Gateway
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
BMC	Broadcast/Multicast Control

BSC	Base Station Controller
BSIC	Base Station Identity Code
BSN	Block Sequence Number
BSS	Base Station Sub-system
BSSAP	BSS Application Part
BSSMAP	BSS Management Application Part
BSSGP	BSS GPRS Protocol
BTS	Base Transceiver Station
BTSM	BTS Management

C

CAMEL	Common Architecture for Enhanced Mobile Logic
CAP	CAMEL Application Part
CBCH	Cell Broadcast CHannel
CCCH	Common Control CHannel
CCTrCH	Coded Composite Transport CHannel
CCU	Channel Codec Unit
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CFI	Control Format Indicator
CG	Charging Gateway
CK	Ciphering Key
CM	Communication Management
CN	Core Network
CPICH	Common Pilot CHannel
CPCH	Common Packet CHannel
CQI	Channel Quality Indicator
CS	Circuit Service
CS	Coding Scheme
CSCF	Call Session Control Function
CTCH	Common Traffic CHannel
CTF	Charging Trigger Function

D

DCCH	Dedicated Control CHannel
DCH	Dedicated CHannel
DCI	Downlink Control Information

DFT	Discrete Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DL-SCH	DownLink Shared CHannel
DNS	Domain Name Service
DPCCH	Dedicated Physical Control CHannel
DPCH	Dedicated Physical CHannel
DPDCH	Dedicated Physical Data CHannel
DRNC	Drift RNC
DRS	Demodulation Reference Signal
DSCH	Downlink Shared CHannel
DTAP	Direct Transfer Application Part
DTCH	Dedicated Traffic CHannel
DTMF	Dual-Tone Multi-Frequency
DTX	Discontinuous Transmission
DwPTS	Downlink Pilot Time Slot

E

E-AGCH	E-DCH Absolute Grant CHannel
E-CSCF	Emergency CSCF
ECSD	Enhanced Circuit-Switched Data
E-DCH	Enhanced Dedicated CHannel
EDGE	Enhanced Data for Global Evolution
E-DPCCH	E-DCH Dedicated Physical Control CHannel
E-DPDCH	E-DCH Dedicated Physical Data CHannel
EFR	Enhanced Full Rate
EGPRS	Enhanced GPRS
E-HICH	E-DCH HARQ Indicator CHannel
EIR	Equipment Identity Register
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-RGCH	E-DCH Relative Grant CHannel
eUTRAN	evolved Universal Terrestrial Radio Access Network

F

FACCH	Fast Associated Control CHannel
FACH	Forward Access CHannel
FCCH	Frequency Correction CHannel

FDD	Frequency Duplex Division
FDMA	Frequency Division Multiple Access
FR	Full Rate

G

GGSN	Gateway GPRS Support Node
GMM	GPRS Mobility Management
GMSC	Gateway MSC
GMSK	Gaussian MSK
GPRS	General Packet Radio Service
GRX	GPRS Roaming eXchange
GSM	Global System for Mobile
GSS	GPRS Sub-System
GT	Global Title
GTP	GPRS Tunnel Protocol
GTP-C	GTP Control
GTP-U	GTP User

H

HARQ	Hybrid Automatic Repeat-reQuest
HLR	Home Location Register
HNB	Home Node B
HNB-GW	HNB Gateway
HR	Half Rate
HSCSD	High-Speed Circuit Switched Data
HS-DPCCH	High-Speed DPCCH
HS-DSCH	High-Speed DSCH
HSN	Hopping Sequence Number
HS-SCCH	High-Speed Shared Control CHannel
HSDPA	High-Speed Downlink Packet Access
HSPA	High-Speed Packet Access
HS-PDSCH	High-Speed PDSCH
HSS	Home Subscriber Server
HSUPA	High-Speed Uplink Packet Access
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol

I

IAD	Integrated Access Device
IAM	Initial Address Message
I-CSCF	Interrogating CSCF
IFFT	Inverse Fast Fourier Transform
IK	Integrity Key
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
INAP	Intelligent Network Application Part
IP	Internet Protocol
IPBCP	IP Bearer Control Protocol
ISIM	IMS Services Identity Module
ISUP	ISDN User Part

L

LAI	Location Area Identification
LAPD	Link Access Protocol – channel D
LAPDm	LAPD mobile
LLC	Logical Link Control
LTE	Long-Term Evolution

M

M3UA	MTP 3 User Adaptation
MAC	Medium Access Control
MAIO	Mobile Allocation Index Offset
MAP	Mobile Application Part
MCCH	Multicast Control Channel
MCH	Multicast Channel
MCS	Modulation and Coding Scheme
ME	Mobile Equipment
MGW	Multimedia Gateway
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
MISO	Multiple Input Single Output
MM	Mobility Management

MME	Mobility Management Entity
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MS	Mobile Station
MSC	Mobile-services Switching Center
MSK	Minimum Shift Keying
MSISDN	Mobile Station ISDN Number
MSRN	Mobile Station Roaming Number
MTCH	Multicast Traffic CHannel
MTP	Message Transfer Part

N

NAS	Non Access Stratum
NBAP	Node B Application Part
NGN	Next Generation Network
NSAPI	Network Service Access Point Identifier
NSS	Network Sub-System

O

OCS	Online Charging System
OFDMA	Orthogonal Frequency-Division Multiple Access
OFDM	Orthogonal Frequency-Division Multiplexing

P

PACCH	Packet Associated Control CHannel
PAGCH	Packet Access Grant CHannel
PBCCH	Packet Broadcast Control CHannel
PCCCH	Packet Common Control CHannel
PCCH	Paging Control CHannel
P-CCPCH	Primary Common Control Physical CHannel
PCEF	Policy and Charging Enforcement Function
PCFICH	Physical Control Format Indicator CHannel
PCH	Paging CHannel
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy-CSCF
PCU	Packet Control Unit

PDCCH	Physical Downlink Control CHannel
PDCH	Packet Data CHannel
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDP	Packet Data Protocol
PDSCH	Physical Downlink Shared CHannel
PDTCH	Packet Data Traffic CHannel
PGW	PDN GateWay
PHICH	Physical HARQ Indicator CHannel
PICH	Paging Indicator CHannel
PLMN	Public Land Mobile Network
PMCH	Physical Multicast Channel
PMI	Precoding Matrix Indicator
PPCH	Packet Paging CHannel
PRACH	Packet Random Access CHannel
PRACH	Physical Random Access CHannel
PS	Packet Service
PSK	Phase Shift Keying
PSS	Primary Synchronization Signal
PSTN	Public Switched Telephone Network
PTCCH	Packet Timing Control CHannel
P-TMSI	Packet-TMSI
PUCCH	Physical Uplink Control CHannel
PUSCH	Physical Uplink Shared CHannel

Q

QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying

R

RAB	Radio Access Bearer
RACH	Random Access CHannel
RADIUS	Remote Authentication Dial In User Service
RAI	Routing Area Identity
RANAP	Radio Access Network Application Part
REL	RELease
RI	Rank Indicator

RLC	ReLease Complete
RLC	Radio Link Control
RLP	Radio Link Protocol
RNC	Radio Network Controller
RNSAP	Radio Network Subsystem Application Part
RNTI	Radio Network Temporary Identity
ROHC	Robust Header Compression
RR	Radio Resource
RRC	Radio Resource Control
RTP	Real-time Transport Protocol
RUA	RANAP User Adaptation

S

S1-AP	S1 Application Part
SACCH	Slow Associated Control CHannel
SAE	System Architecture Evolution
SAPI	Service Access Point Identifier
SCCP	Signaling Connection Control Part
S-CCPCH	Secondary Common Control Physical CHannel
SCH	Synchronization CHannel
SCP	Service Control Point
S-CSCF	Serving-CSCF
SCTP	Stream Control Transmission Protocol
SDCCH	Stand-alone Dedicated Control CHannel
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SF	Spread Factor
SGSN	Service GPRS Support Node
SGW	Signaling GateWay
SGW	Serving GateWay
SIB	System Information Block
SIGTRAN	SIGnaling TRANsport over IP
SIM	Subscriber Identity Module
SIMO	Single Input Multiple Output
SIP	Session Initiation Protocol
SISO	Single Input Single Output
SLF	Subscription Locator Functional
SM	Session Management
SMS	Short Message Service

SNDCP	SubNetwork Dependent Convergence Protocol
SRNC	Serving RNC
SRS	Sounding Reference Signal
SS7	Signaling System 7
SSN	Sub-System Number
SSP	Service Switching Point
SSS	Secondary Synchronization Signal
STP	Signaling Transfer Point

T

TA	Time Advance
TA	Tracking Area
TAI	Tracking Area Identity
TBS	Transport Block Size
TCAP	Transaction Capabilities Application Part
TCH	Traffic CHannel
TCP	Transport Control Protocol
TDD	Time Duplex Division
TDMA	Time Division Multiple Access
TEI	Terminal End point Identifier
TFCI	Transport Format Combination Indicator
TFI	Temporary Flow Identifier
TFI	Transport Format Indicator
TLLI	Temporary Link Layer Identity
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TRAU	Transcoder/Rate Adaptor Unit
TSC	Tandem Switching Center
TTI	Transmission Time Interval

U

UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDI	Unrestricted Digital Information
UDP	User Datagram Protocol
UE	User Equipment

UICC	Universal Integrated Circuit Card
UL-SCH	Uplink Shared CHannel
UMTS	Universal Mobile Telecommunications System
UpPTS	Uplink Pilot Time Slot
URI	Uniform Resource Identifier
USIM	UMTS Subscriber Identity Module
UTRAN	UMTS TRAnsport Network

V

VAD	Voice Activity Detector
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
VLR	Visitor Location Register
VPN	Virtual Private Network

W

WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WP	Wireless Profile
WML	Wireless Markup Language
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol

X

X2-AP	X2 Application Part

Bibliography

Normative references

Recommendations for mobile networks are available on the website for the 3GPP organization (www.3gpp.org) and are arranged into the following series:

Specification series	3G and beyond/GSM (R99 and later)	GSM only (before Rel-4)
Requirements	21 series	01 series
Service aspects	22 series	02 series
Technical realization	23 series	03 series
Signaling protocols User equipment to network	24 series	04 series
Radio aspects	25 series	05 series
CODECs	26 series	06 series
Data	27 series	07 series
Signaling protocols RSS-CN (Radio Sub-system – Core Network) OAM&P and charging (overflow from 32-range)	28 series	08 series
Signaling protocols Intra-fixed-network	29 series	09 series
Program management	30 series	10 series
Subscriber Identity Module (SIM/USIM), IC Cards Test specifications	31 series	11 series
OAM&P and charging	32 series	12 series
Access requirements and test		13 series

Specification series	3G and beyond/GSM (R99 and later)	GSM only (before Rel-4)
specifications		
Security aspects	33 series	-
UE and (U)SIM test specifications	34 series	-
Security algorithms	35 series	-
LTE (Evolved UTRA) and LTE-advanced radio technology	36 series	-
Multiple radio access technology aspects	37 series	-

Specifications for telephone signaling and the gateway command protocol are available on the ITU organization website at: www.itu.int/en/pages/default.aspx:

Q.7xx: Signaling System No. 7 Recommendations

Q.12xx: Intelligent Network Recommendations

Q.19xx: BICC (Bearer Independent Call Control) Recommendations

H.248.x: Gateway Control Protocol Recommendations

Specifications for internet protocol signaling, media transport and signaling transport protocols are available on the Internet Engineering Task Force website (www.ietf.org):

[RFC 3261] – SIP: Session Initiation Protocol, which has been updated by RFC 3853, RFC 4320, RFC 5621, RFC 5393 and RFC 6026

[RFC 3665] – Session Initiation Protocol (SIP), Basic Call Flow Examples

[RFC 3666] – Session Initiation Protocol (SIP), Public Switched Telephone Network (PSTN) Call Flows

[RFC 2327] – SDP: Session Description Protocol, which has been made by RFC 4566

[RFC 1889] – RTP: A Transport Protocol for Real-Time Applications, which has been made obsolete by RFC 3550

[RFC 2719] – Framework Architecture for Signaling Transport

[RFC 3332] – Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA), Superseceded by RFC 4666

[RFC 2960] Stream Control Transmission Protocol, which has been made obsolete by RFC 4960

General Bibliography

[CAM 08] CAMARILLO G., GARCIA-MARTIN M., *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds* (3rd edition), John Wiley & Sons, Chichester, 2008.

[DAH 08] DAHLMAN E., PARKVALL S., SKÖLD J., BEMING P., *3G Evolution: HSPA and LTE for Mobile Broadband*, Academic Press, 2008.

[EBE 09] EBERSPÄCHER J., VÖGEL H-J., BETTSTETTER CK., HARTMANN C., *GSM: Architecture, Protocols and Services*, John Wiley & Sons, Chichester, 2009.

[HOL 06] HOLMA H., TOSKALA A., *HSDPA/HSUPA for UMTS: High Speed Radio Access for Mobile Communications*, Wiley-Blackwell, 2006.

[KAA 06] KAARANEN H., AHTIAINEN A., LAITINEN L., NAGHIAN S., NIEMI V., *UMTS Networks: Architecture, Mobility and Services*, Wiley-Blackwell, 2005.

[LAG 00] LAGRANGE X., GODLEWSKI P., TABBANE S., *Réseaux GSM-DCS*, Hermès-Lavoisier, Paris, France, 2000.

[LES 02] LESCUYER P., *UMTS: Les Origines, l'Architecture et la Norme*, Dunod, Paris, France, 2002.

[LES 08] LESCUYER P., LUCIDARME T., *Evolved Packet System (EPS): The LTE and SAE Evolution of 3G UMTS*, Wiley-Blackwell, 2008.

[POI 09] POIKSELKA M., MAYER G., KHARTABIL H., NIEMI A., *The IMS: IP Multimedia Concepts and Services*, Wiley-Blackwell, 2009.

[SAN 03] SANDERS G., THORENS L., REISKY M., RULIK O., DEYLITZ S., *GPRS Networks*, John Wiley & Sons, Chichester, 2003.

[SEU 03] SEURRE E., SAVELLI P., PIETRI P-J., *EDGE for Mobile Internet*, Artech House, Norwood, USA, 2003.

Index

A

access, 1-2, 5, 10-11, 22-27, 38, 49, 105-110, 113-117, 121-124, 131-132, 138-141, 145, 148, 155-160, 166-167, 175-176, 179-185, 190-191, 203, 207-211, 216-217, 224, 227, 240, 249
  network, 1, 53, 105-107, 114, 156-160, 166-167, 176, 224
acknowledged mode, 58, 76, 80, 84, 119, 186
AGCH, 20, 23, 28-29, 32-33, 37-38, 73, 89-91
AICH, 124, 131-132
AMR, 106, 122, 160
AN, 220- 224
antenna, 5, 151-154, 189-190, 199, 204, 209
APM, 163-166
APN, 57, 62, 67, 87
architecture, 1-6, 10, 16, 53, 56-60, 105-109, 115, 155-157, 175-178, 227, 236
area, 4, 72, 85, 117, 176, 187
AS (Access Stratum), 110, 138
AS (Application Server), 236, 239
attach, 60-63, 85-87
attachment, 53, 85, 93, 177-180, 187, 211
AuC, 4, 13-15, 39-40, 159, 177
authentication, 4, 7, 14, 39-46, 57, 65, 86, 93-94, 110, 159, 176-177, 180, 212-216, 229, 238, 240, 243-244

B

B2BUA, 229
bandwidth, 64, 97, 124, 132, 135, 182-183, 191-192, 198
BCCH, 20, 23, 27-28, 32-35, 42, 71-72, 117, 120, 132, 182
BCH, 27, 31, 121-122, 129, 182-183, 203
BCTP, 163-164
beacon, 27-33, 41-42, 48
bearer service, 2, 106, 109
BGCF, 236, 239-241
BICC, 163-167, 172
BMC, 113-114, 119
BSC, 4-6, 10-11, 15, 37-38, 41, 45-51, 59, 61, 68, 75, 96, 107, 156, 161-162, 166-168, 171, 177
BSIC, 27, 28, 35

BSS, 1-3, 6, 10-11, 36, 43, 46-56, 59, 61, 69, 86, 93, 96, 155-158
BSSAP, 11, 86, 95, 156, 166
BSSMAP, 11, 37, 41, 45, 50-51, 56, 59, 60, 156
BTS, 4-6, 10-22, 24-29, 35-42, 48-49, 54, 68-69, 73, 96, 102, 184
BTSM, 10-11, 37-38, 41, 48-49
burst, 21-31, 35-37, 49, 70, 73, 97

C

call, 2-4, 8-15, 22, 28-29, 37-38, 42- 47, 87, 91-92, 110, 124, 156, 157, 163, 166, 216-217, 223, 228- 231, 234-236
  incoming –l, 6, 14, 37-38, 42-46, 73, 117, 166-167, 217, 232, 238-239
  outgoing –, 1, 15, 36-39, 42-47, 155, 164-165, 216, 239
CAMEL, 16, 159
CAP, 16, 159
carrier, 5, 29, 54, 96, 132, 190-191, 198, 200
CCCH, 28, 120, 138, 183-184, 211
ccess, 53, 57-61, 64, 68, 72-75, 78, 84-85, 89-90
CCU, 54, 69
CDF, 242
CDMA, 132, 135-136
cell, 4, 26-29, 32-34, 39-42, 47-50, 63, 72-73, 89-93, 112-118, 121-123, 128, 132, 135-136, 168, 171, 178, 181-187, 193, 199-201, 204, 209, 214, 220-224
CELL_DCH state, 116
CELL_FACH state, 117, 140
CELL_PCH state, 116
CG, 177
channel, 1, 6, 10-11, 17-33, 36-38, 42, 47-50, 53-55, 58, 68-74, 89- 92, 97, 115, 120-137, 143, 146- 152, 160, 181-186, 189, 192-194, 198-199, 204-211
  coding, 1, 17-19, 20, 53-55, 68-70, 97, 122-125, 143
channelization code, 127-134, 146, 150
charging, 57, 176-177, 180-181, 237- 243, 246, 249
chip, 132, 137
circuit mode, 54-58, 95, 106
CK, 185, 204, 244
CM, 8-11, 37, 44-46, 110, 114, 156-157, 164-167
CN, 140-142
code, 5, 16-20, 27-28, 35, 112, 125- 128, 131-137, 145-148, 153, 159, 182, 196, 201, 204, 231, 234
codec, 18-20, 30, 54, 106, 122, 157, 160-161, 172, 227-228, 248-249
coding, 1, 17-22, 30, 69-71, 98-99, 102-103, 122, 145, 148, 186, 189, 190, 201, 204-205, 209-210
  rate, 99, 103, 122, 145, 204-205, 209-210
  scheme, 98-99, 103, 186
common control, 28, 71-72
compression, 59, 64, 68, 81-83, 114, 178, 185
concatenation, 53, 105, 119, 186
connected state, 116, 185-187, 216
connection, 4, 8-13, 16, 37, 45-52, 60- 61, 65, 78-82, 107, 115-116, 120-124, 138-141, 144, 157-162, 166, 169-177, 184-185, 211-212, 216-217, 245-246
control, 1-2, 6, 11-17, 22-24, 28-29, 52, 56-60, 68, 71-80, 99-102, 106-130, 134-136, 140, 143, 146-147, 150-164, 178-187, 198-208, 227, 236-241, 248-249
  plane, 110-113, 179, 187
convolutional code, 19-21, 27-28, 69-70, 98, 102, 122, 125, 129-131

core network, 1, 53, 105-107, 110, 115-117, 138-142, 155, 176, 185
CPCH, 122
CPICH, 124, 128-129
CS (Circuit Service), 1, 105, 110, 155, 223
CS (Coding Scheme), 98-99, 103, 186
CSCF, 236- 240, 243-251
CTCH, 120
CTF, 242
cyclic
  code, 19, 196
  prefix, 196-198, 201, 208-209

D

data
  network, 2, 13, 56-59, 65
  transmission, 1-2, 53-54, 63, 73, 105, 116, 119, 175, 176
database, 12-13, 40, 156, 177, 212, 240-242
DCCH, 29, 117, 120-121, 138-141, 183-184, 212
DCH, 116-118, 121-122, 140, 146, 149-150
dedicated control, 33, 72-73
detach, 60-63, 86
detachment, 53, 86-87, 177
DFT, 191-192
DIAMETER, 180-181, 212- 215, 242
discontinuous transmission, 19, 146, 183
DL-SCH, 182-184
DPCCH, 126-127, 134
DPCH, 126-127
DPDCH, 126-127, 133-134, 150
DRNC, 107-110, 141
DRS, 207- 211
DSCH, 121-122, 127
DTAP, 11
DTCH, 120-121
DTCH, 183-184
DTMF, 2, 9
DTX, 19
DwPTS, 194

E

E-CSCF, 238-239
ECSD, 95
E-DCH, 149- 151
EDGE, 53, 95-96
E-DPCCH, 150
E-DPDCH, 150
EFR, 6, 18- 21, 30
EGPRS, 95-96, 99-103, 106
E-HICH, 150
EIR, 4, 13-15, 159, 176, 181
encryption, 6-7, 17, 22, 39-46, 49, 59, 68-69, 78-81, 86, 93-94, 109-110, 119-121, 176-178, 184-185
eNode B, 177-181, 184-188, 193-194, 202-203, 209-214, 217- 224
EPC, 175-176
EPS, 175-178, 223-225, 236, 243, 246
establishment, 1, 4-12, 22, 29, 36-39, 45- 49, 53-54, 80-82, 89-92, 105, 112-115, 122, 138-144, 155-157, 163-167, 170, 173-175, 179-180, 184, 187, 211-217, 227-230, 238, 244, 250
eUTRAN, 175-179, 187, 220-222

F

FACCH, 20, 23, 29-31, 48-49, 71-73
FACH, 116-118, 121-122, 130, 138
FCCH, 23, 27, 32-33, 42, 71
FDD, 135, 192-194, 199-202, 209
FDMA, 5, 191-192
femtocell, 114-115
FR, 6, 18- 21, 30, 60

frame, 4, 10-11, 22, 26-27, 30-37, 49, 56, 60-61, 69-73, 76-81, 84, 97-98, 109, 119-120, 125-130, 137, 143- 152, 160, 181-182, 194-196, 199, 201-204, 208-209
  frame duration, 150
frequency band, 5-6, 34-35, 135, 192-194, 205-206, 210

G

gateway, 4, 16, 56-58, 64- 67, 87, 156, 161-162, 168, 176-177, 228-229, 236, 242, 251
GGSN, 56- 64, 67, 81, 86-88, 94, 176-177, 236
GMM, 61, 80-81, 86, 89, 93, 96, 110, 114
GMSC, 4, 12-15, 44-45, 156-157, 166, 167
  Server, 156-157, 166-167
GMSK, 34, 68, 96-98
GPRS, 53-64, 67, 71-73, 82, 85-87, 93-96, 99-110, 116, 138, 155, 175-176, 179, 184, 223-224, 236
GRX, 67
GSM, 1-5, 13, 34-35, 42, 53- 62, 68-73, 85-87, 93-97, 105-110, 116, 135, 138, 143-144, 166, 175, 183-184, 223
GSS, 53-56, 105-107, 115, 138, 155, 176
GTP, 57- 60, 86-88, 93-94, 115, 179-181, 187, 213-214, 217-221, 224
  -C, 180, 213-214, 217-221, 224
  -U, 179-181, 187
guard time, 24-25, 196, 209

H

H.248, 161-164, 170
handover, 4, 6-7, 11-12, 15, 23, 27-29, 47-51, 93, 105-110, 118, 141- 144, 155, 168-175, 179-181, 184- 188, 211, 220-225
HARQ, 147, 150, 182-186, 199, 202-204
HLR, 4, 12-15, 39-45, 56, 57, 60, 62, 86-88, 93, 94, 156, 159, 166, 177
HNB, 114-115
  -GW, 114-115
HR, 6, 18-20, 30
HSCSD, 54, 55
HSDPA, 145, 148, 151
HS-DPCCH, 147, 151-153
  -DSCH, 145-146
  -PDSCH, 146
  -SCCH, 146-147, 151-153
HSPA, 105, 145, 151
HSS, 176-177, 180, 185, 212-215, 236-240, 243-248
HSUPA, 148, 151

I

I-CSCF, 237-239, 243-246
identifier, 10-11, 42, 56, 61-62, 75-77, 80-81, 89-90, 93, 110, 118, 146, 152, 161-162, 177, 185, 230-231
identity, 4-7, 12-15, 27-29, 37-39, 42, 45, 56, 60-62, 72, 85-86, 109, 117, 123, 159-161, 166, 176, 182, 185, 200, 211, 214, 230, 240, 243-245
IDLE state, 63-64
IFFT, 190-192
IK, 185, 244
IMEI, 5, 13, 181
IMS, 175-177, 227, 236-244, 251
IMSI, 5, 8, 12-13, 37-45, 56, 62, 85-88, 94, 176, 212
INAP, 13-16
incremental redundancy, 103, 147, 186
integrity, 65, 184-185, 244
intelligent network, 15, 159

interleaving, 21-22, 68-70, 102
Internet, 53, 56, 64-66, 106, 114, 155, 177, 228
IP, 56-59, 62-68, 81-83, 88, 106, 114-115, 155-168, 172, 175-184, 187, 214, 222, 227-239, 243-247
IPBCP, 163-166, 172
ISIM, 243-244
ISUP, 13-14, 44-46, 51-52, 156, 159, 163, 166

L, M

LAI, 4, 12, 28, 38, 42-43, 85-86
LAPD, 11
LAPDm, 10-11, 32, 37
LLC, 58-61, 68-69, 73-84, 94-96, 101, 103
location, 1, 4-8, 11-15, 28-29, 36, 39, 41-45, 53, 56, 62-64, 85-87, 93-95, 116-118, 131, 139, 156, 175-177, 182, 187, 211-215, 228-229, 232, 239
  larea, 11, 42, 45, 62, 117, 177
  service, 228-229, 232
logical channel, 1, 10, 20-23, 27-28, 53-54, 59, 69-73, 89-92, 113, 120-123, 139, 149, 152, 181-184
LTE, 176
M3UA, 158-159
MAC, 59, 68-70, 73-77, 96-102, 113-115, 120-125, 145-146, 149, 152-153, 181, 184-186
MAP, 13-15, 40, 43-45, 51-52, 56-57, 60, 86-88, 94, 158, 172-173
MCCH, 183
MCH, 183-184
MCS, 98-103
ME, 109
MIMO, 151, 154, 189-190
MISO, 189
MM, 4, 7-13, 37, 40-43, 110, 114, 155-157
MME, 176-181, 184-187, 211-224
mobility, 3-4, 56, 61- 63, 78, 86-87, 91-94, 110-112, 116-118, 155, 176-179, 220
  context, 62, 86-87, 91-94
mode, 1-5, 10-11, 16, 19, 28, 36, 41, 49, 53-54, 57-58, 65, 79-80, 84, 105-106, 109, 115-116, 120, 130-132, 135, 139, 143, 151, 155, 159, 175-176, 182, 186, 189-195, 199, 200-202, 209, 223, 227, 236, 240
modulation, 1, 5, 18, 34, 53, 69, 96-98, 105, 123, 134-135, 145-148, 151, 186, 191, 201-205, 208-210
MRFC, 236, 241
MRFP, 241
MS, 1-6, 12, 35, 40-44, 49, 69, 78, 82-83, 87
MSC, 4-15, 37-56, 60, 86-87, 95, 107, 110, 114, 126, 143-144, 155-173
  Server, 155-173
MSISDN, 12-13, 44, 94
MSK, 34
MSRN, 12, 45, 51
MTCH, 183
MTP, 16, 158
multiple access, 132
multiplexing, 30-33, 82, 134, 160, 190, 205-206, 210

N, O

NAS, 110, 115, 138-139, 179, 184-187, 211-219
NBAP, 110-111, 140
network, 1-6, 11-13, 16-17, 22, 26-29, 34, 39-49, 53-67, 71-72, 75, 83-96, 105-118, 123, 131, 140-144, 151, 155-168, 172, 175- 185, 212, 223-224, 227, 233, 236- 250
NGN, 155-158, 167

node B, 107-115, 127, 131-133, 136-137, 140-141, 145, 148-153, 184
NSAPI, 61-62, 68, 81-85
NSS, 1, 4-6, 12, 105-107, 138
OCS, 242, 251
OFDM, 190-192, 196, 199-200, 203-204
OFDMA, 190-192

P

PACCH, 72-73, 89-90
packet mode, 58, 95, 106
PAGCH, 72-73, 89-91
paging, 6-7, 23, 38, 42, 45, 72-73, 87, 91-92, 110-113, 117, 120-121, 124, 130, 138-140, 177-178, 183- 187, 203, 217
PBCCH, 71-72
PCCCH, 71
PCCH, 117, 120, 139, 183
P-CCPCH, 129
PCEF, 177, 181, 218, 249
PCFICH, 199-206
PCH, 20, 23, 28-29, 32-33, 38, 42, 45, 92, 116-118, 121-122, 130, 139, 183
PCRF, 176-177, 180-181, 218-219, 246, 248-251
P-CSCF, 237-239, 243-251
PCU, 56, 68-69, 73
PDCCH, 148, 185, 199, 203-206
PDCH, 72-73, 89, 91
PDCP, 113-115, 119, 185-186
PDN, 53, 176, 177, 181, 236
PDP, 56, 60-62, 81-82, 86-89, 94
  context, 56, 60-62, 81-82, 86-89, 94
PDSCH, 127, 146, 183-184, 199, 203-206
PDTCH, 72
PGW, 176-177, 214-219, 223-224
PHICH, 182, 199, 202, 206
physical
  architecture, 5, 12
  channel, 22, 26, 29, 32, 105, 118, 124-125, 130, 175, 181-182, 198-199, 205-210
  signal, 198-200, 206-207
PICH, 124, 130
pilot, 126, 130, 137, 154, 194
plane, 110-113, 179, 187, 217
PLMN, 1, 3, 12, 44, 155-156, 160, 236, 240-241
PMCH, 184, 199
power control, 6, 29, 72, 126, 131, 136-137, 145, 148, 183
PPCH, 72-73, 92
PRACH, 72-73, 89, 92, 131-132, 184, 207-210
privacy, 40, 65, 81
protocol architecture, 1, 13, 59, 96, 155, 158
proxy server, 229-240
PS, 53, 105-107, 110-111, 115, 175-176, 223, 227, 236
pseudo-random sequence, 132-134, 200
PSK, 96-98
PSS, 199-201, 205-207
PSTN, 1, 12, 44, 155-156, 160, 227, 236, 240-241
PTCCH, 71-73, 89
P-TMSI, 61-62, 73, 85-86, 93
PUCCH, 184, 204, 207-211
puncturing, 70, 98-99, 102-103, 125, 143, 147, 204
PUSCH, 184, 207-210

Q, R

QAM, 145-147, 151, 204-205, 210
QPSK, 134, 145-147, 151, 201, 204, 208

quality of service (QoS) , 42, 54, 62, 87-88, 106, 176-181
RAB, 106, 109-110, 115, 140-141
RACH, 20, 23, 28-29, 34-38, 42, 46, 73, 89, 92, 117-118, 122, 131-132, 138-139, 184, 211
radio
  channel, 6-7, 11, 21, 37-39, 53-54, 58-59, 95, 108, 122, 137, 151-154, 182-186, 189, 192-194, 198, 206-207
  resource, 3, 53-56, 68, 107-109, 113, 144, 175, 178, 185-188, 207, 217, 222-224
RAI, 72, 85, 86
RAKE, 108, 124, 128, 137-138
RANAP, 110, 115, 139-144, 156-157, 166, 170-173
random access, 28-29, 89-92, 121, 131, 183-184, 207, 211, 216-217
rate, 2, 4-6, 18, 27-31, 34-36, 53-56, 66, 90, 95-99, 105-106, 118, 122, 125-133, 136, 145-151, 159-160, 175, 184-186, 189-190, 201, 204-205, 209-210, 222
READY state, 63, 86, 91
redirect server, 229, 240
registrar, 228, 238-239
registration, 8, 115-117, 131, 211-213, 227-229, 238-240, 243-248
release, 6-14, 43-45, 50-52, 63, 82, 113, 142-144, 155-157, 167-170, 174, 184, 187-188, 220-224, 240
relocation, 105, 141-143, 180, 220- 222
resource elements, 200-206
RLC, 59-61, 64, 68-70, 73-81, 89-90, 96-103, 113-115, 118-121, 145-149, 167, 181, 184-186
RLP, 2
RNC, 107-115, 118-119, 126, 133, 137-145, 149, 157, 162, 166-174, 177, 181, 223
RNSAP, 110-112, 141
RNTI, 118, 123, 138, 185, 204, 211
roaming, 1, 4, 12-14, 53, 56, 60, 67-68, 85, 187
ROHC, 185
routing area, 63, 86, 91-94
RR, 6-7, 10-11, 36-38, 41-42, 45, 48-51, 79
RRC, 96, 109, 113-119, 138-141, 144, 178, 183-185, 211-221
RTP, 115, 160-162
RUA, 115

S

S1-AP, 179, 187, 214-224
SACCH, 20, 23, 29-34
SAE, 176
SAPI, 10-11, 61, 68, 78-83, 113
SCCP, 13, 16, 37, 139, 159
S-CCPCH, 130
SC-FDMA, 191-192
SCH, 20, 23, 27, 32-33, 42, 71, 124, 128-129, 182-184
scheduling, 145, 148-149, 184, 186, 199, 208
SCP, 15
scrambling code, 128-129, 132-135
S-CSCF, 237-248
SCTP, 115, 158, 159
SDCCH, 20, 23, 29, 32, 36-38, 42-48
SDP, 227-228, 231-234, 248-250
security, 8, 15, 28, 39-41, 64-65, 113, 184-187, 216, 230, 238, 244
segmentation, 59, 66-68, 83-84, 103, 119, 125, 152, 186, 204
sequence, 17, 24, 36, 69, 76-79, 84-85, 99-102, 119, 128, 132, 146, 149-152, 159, 185, 200-204, 207

session, 53, 57, 60-61, 65, 78, 87, 110, 116, 159, 175-180, 211, 215, 227-240, 246-253
SF, 127-130, 133, 143-145, 148-150
SGSN, 56-63, 67-68, 78, 83-88, 93- 96, 107, 110, 114, 126, 176-177, 180, 223, 224
SGW, 155-159, 176-181, 214-224, 236
signaling, 1, 4, 10-17, 20-24, 29, 44- 45, 59-61, 68, 73, 78, 89, 105-107, 110-115, 126, 130-131, 138-139, 148, 155-159, 163, 166, 175-187, 199, 207, 211-217, 222-224, 227, 236
network, 13
SIGTRAN, 158
SIM, 4-5, 40
SIMO, 189-190
SIP, 227-234, 237-241, 250
SISO, 151, 189
SLF, 236, 240
slot, 4, 22-23, 26-33, 37, 55, 58, 71, 89, 99, 128-130, 181, 194-203, 206
SM, 61, 78, 82, 88, 96, 110, 114
SMS, 3-4, 8, 12, 29, 32, 56, 61, 68, 78-80, 114
SNDCP, 59-61, 68, 78-85, 96
soft handover, 105, 109, 113, 141, 145, 148
softer handover, 108-109, 112
spreading, 21, 127-128, 131-134, 143-148, 153, 196
factor, 127, 133, 145-148
sequence, 128
SRNC, 107-110, 141-144
SRS, 207-210
SS7, 60, 158-159
SSP, 15
SSS, 199-201, 205-207
STANDBY state, 63, 91-92
state, 62-63, 69, 96, 116, 120, 149, 185-187, 211, 215-216
STP, 17
sub-carrier, 188-194, 197-201
sub-system, 1-5, 12-13, 53, 96, 105-107, 155, 175
switch, 12-15, 41, 50, 63, 143
switching, 4, 15, 54, 107, 155
symbol, 96-97, 123, 145, 194-205, 208
synchronization, 4, 22-27, 71, 124, 128, 135, 151, 199-201, 209-211, 220
system information, 6-7, 22, 27-28, 32, 71, 113, 118-121, 182-184, 199, 203

T

TA, 25-29, 37, 49, 73, 92, 187, 211, 214-215
TAI, 89, 176-177, 182
TCAP, 14-16
TCH, 20, 23, 29-30, 36-37, 44, 48, 54-55, 71-72
TCP, 59, 64-67, 82-83, 106, 114, 159-160, 222
TDD, 182, 192-196, 199-202, 209
TDMA, 5, 10, 22, 27
TEI, 11
telephone service, 1, 105, 163, 175-177, 227
teleservice, 2-3, 106
TFCI, 124-127, 130, 150
TFI, 61, 73-77, 89-91, 100-101
time advance, 73
time-slot, 4-6, 10, 17, 21-22, 27, 37, 137, 143, 146-147, 161-162, 181, 194-200, 203, 206
TLLI, 61-62, 76-81, 89-92
TLS, 64-65, 230
TMSI, , 7-8, 12, 37-39, 42-44, 61, 85-86
traffic
channel, 4, 20, 31, 45-46, 113, 126, 181, 206

traffic plane, 115, 179, 187, 217
training sequence, 24-29, 35, 97
transcoding, 4-6, 157, 241
transit network, 67
transmission network, 4, 17, 155
transmission, 1-5, 8-12, 17-21, 24-26, 30-32, 36, 39-40, 45, 50, 53, 58, 68-69, 73-76, 86, 105, 109, 113, 116-124, 127-132, 135-137, 143-159, 167, 175-178, 181-186, 189, 192-194, 209, 215, 229
transmit diversity, 129-130, 189
transparent mode, 2, 57, 119-121, 186
transport channel, 113, 117-132, 146, 149, 181-183, 199, 204, 207
TRAU, 4-6
TSC, 4, 12, 46
tunnel, 57-62, 67, 94, 177-180, 224
tunnelization, 163-164
turbo code, 122, 143, 204

U, W, X, Z

UA, 80, 228-238
UAC, 228-229, 240
UAS, 228-229, 240
UDI, 2, 106
UDP, 59-60, 65, 83, 115, 160, 163, 222, 230, 234
UE, 107-109, 123, 139, 175, 216, 237-239, 243, 246-251
UICC, 109, 243
UL-SCH, 183-184
UMTS, 105-109, 114-116, 135, 143-149, 152, 155, 160, 168-177, 183-184, 212, 223-225, 236, 243, 246
unacknowledged mode, 58, 80, 84-85, 90, 119, 186
UpPTS, 194, 209
URA_PCH state, 116-117, 139
URI, 230-231, 234, 237-239, 246
user plane, 110-114, 126
UTRAN, 105-109, 117-118, 123, 140-141, 144, 156, 159-160, 170, 174
VLR, 4, 12-15, 39-45, 51
WAE, 64
WAP, 64-67
WDP, 65
WSP, 65
WTLS, 65
WTP, 65
X2-AP, 181, 187, 220
Zadoff-Chu sequence, 200, 207