NETWORKS & TELECOMMUNICATIONS SERIES

LTE Advanced Pro

Towards the 5G Mobile Network

Frédéric Launay

André Perez

ISTE

WILEY

LTE Advanced Pro

LTE Advanced Pro

Towards the 5G Mobile Network

Frédéric Launay
André Perez

ISTE
WILEY

First published 2019 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 Control Number: 2019933515

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78630-430-8

Contents

List of Abbreviations

3GPP:	3rd Generation Partnership Project
5GC:	5G Core
5G NR:	5G New Radio

A

AA:	Antenna Array
AAA:	Authentication, Authorization and Accounting
AAA:	Authenticate-Authorize-Answer
AAR:	Authenticate-Authorize-Request
AAS:	Active Antenna System
ADM:	Activation/Deactivation MAC
AES:	Advanced Encryption Standard
AESE:	Architecture Enhancements for Service capability Exposure
AF:	Application Function
AH:	Authentication Header
AIA:	Authentication-Information-Answer
AIR:	Authentication-Information-Request
AKA:	Authentication and Key Agreement

AM:	Acknowledged Mode
AMBR:	Aggregate Maximum Bit Rate
ANDI:	Access Network Discovery Information
ANDSF:	Access Network Discovery and Selection Function
ANQP:	Access Network Query Protocol
AP:	Access Point
AP:	Application Part
API:	Application Programming Interface
APN:	Access Point Name
ARP:	Allocation and Retention Priority
ARQ:	Automatic Repeat reQuest
AS:	Application Server
ASA:	Abort-Session-Answer
ASR:	Abort-Session-Request
AUTN:	Authentication Network

B

BBU:	Base Band Unit
BCE:	Binding Cache Entry
BIA:	Bootstrapping-Info-Answer
BIR:	Bootstrapping-Info-Request
BM-SC:	Broadcast/Multicast Service Center
BSF:	Bootstrapping Server Function
BSSID:	Basic Service Set Identifier
B-TID:	Bootstrapping Transaction Identifier
BWP:	Bandwidth Part

C

CA:	Carrier Aggregation
CC:	Component Carrier
CCA:	Clear Channel Assessment
CCA:	Credit-Control-Answer
CCR:	Credit-Control-Request
CDD:	Cyclic Delay Diversity
CE:	Coverage Extension
CIA:	Configuration-Information-Answer
CIoT:	Cellular Internet of Things
CIR:	Configuration-Information-Request
CK:	Cipher Key
CMA:	Connection-Management-Answer
CMR:	Connection-Management-Request
CN:	Correspondent Node
CNA:	Correspondent Node Address
CoA:	Care of Address
CoMP:	Coordinated Multi Point
CP:	Control Plane
CPRI:	Common Public Radio Interface
CQI:	Channel Quality Indicator
CRC:	Cyclic Redundancy Check
CRI:	CSI Resource Index
CRS:	Cell-specific Reference Signal
CS:	Circuit-Switched
CSFB:	Circuit-Switched Fallback
CSI:	Channel State Information

CSMA/CA:	Carrier Sense Multiple Access/Collision Avoidance
CU:	Centralized Unit
CUPS:	Control and User Plane Separation

D

D2D:	Device to Device
DAA:	Device-Action-Answer
DAR:	Device-Action-Request
DC:	Dual Connectivity
DCI:	Downlink Control Information
DEA:	Diameter-EAP-Answer
DeNB:	Donor eNB
DER:	Diameter-EAP-Request
DFT-S-OFDM:	Discrete Fourier Transform Spread OFDM
D–H:	Diffie–Hellman
DHCP:	Dynamic Host Configuration Protocol
DL:	Downlink
DL-SCH:	Downlink Shared Channel
DMRS:	Demodulation Reference Signal
DMTC:	Discovery Measurement Timing Configuration
DNA:	Device-Notification-Answer
DNR:	Device-Notification-Request
DNS:	Domain Name System
DoA:	Direction of Arrivals
DRA:	Device-Report-Answer
DRB:	Data Radio Bearer
DRR:	Device-Report-Request
DRS:	Discovery Reference Signal

DSCP: DiffServ Code Point

DSMIPv6: Dual-Stack Mobile IP version 6

DTA: Device-Trigger-Answer

DTR: Device-Trigger-Request

DU: Distributed Unit

DwPTS: Downlink Pilot Time Slot

E

EAP: Extensible Authentication Protocol

EAPOL: EAP Over LAN

EBF: Elevation Beamforming

ECGI: E-UTRAN Cell Global Identifier

eCPRI: enhanced Common Public Radio Interface

eDRX: extended Discontinuous Reception

EHSP: Equivalent Home Service Providers

eICIC: enhanced Inter-Cell Interference Coordination

eLAA: enhanced LAA

eMBMS: evolved Multimedia Broadcast/Multicast Service

EMSK: Extended Master Session Key

eNB: evolved Node Base station

en-gNB: E-UTRA-NR DC next generation Node B

EPC: Evolved Packet Core

ePDCCH: enhanced PDCCH

ePDG: evolved Packet Data Gateway

EPS: Evolved Packet System

E-RAB: EPS Radio Access Bearer

ESP: Encapsulating Security Payload

E-UTRAN: Evolved Universal Terrestrial Radio Access Network

F

FA:	Foreign Agent
FAA:	Foreign Agent Address
FBE:	Frame-Based Equipment
FDD:	Frequency-Division Duplex
FD-MIMO:	Full-Dimension MIMO
FEC:	Forward Error Correction
FFT:	Fast Fourier Transform
FLUTE:	File Delivery over Unidirectional Transport
FQDN:	Full Qualified Domain Name
FR:	Frequency Range
FSTD:	Frequency Shift Transmit Diversity

G

GAA:	GCS-Action-Answer
GAR:	GCS-Action-Request
GAS:	Generic Advertisement Service
GBA:	Generic Bootstrapping Architecture
GCSE:	Group Communication System Enablers
GNA:	GCS-Notification-Answer
gNB:	next generation Node Base station
GNR:	GCS-Notification-Request
GNSS:	Global Navigation Satellite System
GP:	Gap Period
GRE:	Generic Routing Encapsulation
GTP-U:	GPRS Tunneling Protocol User
GTPv2-C:	GPRS Tunneling Protocol Control
GUTI:	Globally Unique Temporary Identity

H

HA:	Home Agent
HARQ:	Hybrid Automatic Repeat reQuest
HeNB:	Home eNB
HESSID:	Homogeneous Extended Service Set Identifier
HI:	HARQ Indicator
HNP:	Home Network Prefix
HoA:	Home Address
HSS:	Home Subscriber Server
HTTP:	Hypertext Transfer Protocol

I

IARP:	Inter-APN Routing Policy
ICE:	Interactive Connectivity Establishment
IDA:	Insert-Subscriber-Data-Answer
IDR:	Insert-Subscriber-Data-Request
IEEE:	Institute of Electrical and Electronics Engineers
IFFT:	Inverse Fast Fourier Transform
IFOM:	IP Flow Mobility
IGMP:	Internet Group Management Protocol
IK:	Integrity Key
IKEv2:	Internet Key Exchange version 2
IMS:	IP Multimedia Sub-system
IMSI:	International Mobile Subscriber Identity
IP:	Internet Protocol
IPSec:	IP Security

IP-SM-GW: IP Short-Messaging Gateway

ISMP: Inter-System Mobility Policy

ISRP: Inter-System Routing Policy

L

LAA: Licensed Assisted Access

LAPI: Low Access Priority Indicator

LBE: Load-Based Equipment

LBT: Listen Before Talk

LCID: Logical Channel Identifier

LDPC: Low-Density Parity Check

LLC: Low Latency Communication

LLC: Logical Link Control

LMA: Local Mobility Anchor

LMAA: LMA Address

LMD: Local Mobility Domain

LTE: Long-Term Evolution

LWA: LTE–Wi-Fi Aggregation

LWAAP: LWA Adaptation Protocol

LWIP: LTE/WLAN radio level integration with IPsec tunnel

LWIPEP: LWIP Encapsulation Protocol

M

MAA: Multimedia-Authentication-Answer

MAC: Medium Access Control

MAC: Message Authentication Code

MAG: Mobile Access Gateway

MAPCON: Multi-Access PDN Connectivity

MAR:	Multimedia-Authentication-Request
MBB:	Mobile Broadband
MBMS GW:	MBMS Gateway
MBSFN:	MBMS Single-Frequency Network
MCC:	Mobile Country Code
MCCH:	Multicast Control Channel
MCE:	Multi-cell/Multicast Coordination Entity
MCG:	Master Cell Group
MCH:	Multicast Channel
MCL:	Maximum Coupling Loss
MCM:	Multi-Connection Mode
MCPTT:	Mission Critical Push-to-Talk
MCS:	Modulation and Coding Scheme
MEC:	Mobile Edge Computing
MeNB:	Master eNB
MIB:	Master Information Block
MIB-NB:	MIB NarrowBand
MIKEY:	Multimedia Internet KEYing
MIMO:	Multiple Input Multiple Output
MIP:	Mobile IP
MIP-RK:	MIP Root Key
MIPv4 FA:	Mobile IP version 4 Foreign Agent
MISO:	Multiple Input Single Output
MLP:	Mobile Location Protocol
MME:	Mobility Management Entity
MN:	Mobile Node
MNC:	Mobile Network Code

MO: Management Object
MPDCCH: MTC PDCCH
MRK: MBMS Request Key
MSC: Mobile Switching Center
MSK: Master Session Key
MSK: MBMS Service Key
MTC: Machine Type Communication
MTCH: Multicast Traffic Channel
MTK: MBMS Traffic Key
MUK: MBMS User Key
MU-MIMO: Multi-User MIMO

N

NAI: Network Access Identifier
NAPT: Network Address and Port Translation
NAS: Non-Access Stratum
NAT: Network Address Translation
NB-IoT: NarrowBand Internet of Things
NCCE: Narrowband Control Channel Element
NFV: Network Function Virtualization
NIA: NIDD-Information-Answer
NIDD: Non-IP Data Delivery
NIR: NIDD-Information-Request
NPBCH: Narrowband PBCH
NPDCCH: Narrowband PDCCH
NPDSCH: Narrowband PDSCH
NPRACH: Narrowband PRACH
NPSS: Narrowband PSS

NPUSCH: Narrowband PUSCH

NRS: Narrowband Reference Signal

NSA: Non-Standalone

NSSS: Narrowband SSS

NSWO: Non-Seamless WLAN Offload

O

OCC: Orthogonal Covering Code

ODA: MO-Data-Answer

ODR: MO-Data-Request

OFDM: Orthogonal Frequency-Division Multiplexing

OFDMA: Orthogonal Frequency-Division Multiple Access

OPI: Offload Preference Indication

OTDOA: Observed Time Difference Of Arrival

P

PBA: Proxy Binding Acknowledgment

PBCH: Physical Broadcast Channel

PBU: Proxy Binding Update

PCCC: Parallel Concatenated Convolutional Code

PCEF: Policy and Charging Enforcement Function

PCFICH: Physical Control Format Indicator Channel

PCI: Physical-layer Cell Identity

PCRF: Policy and Charging Rules Function

PDCCH: Physical Downlink Control Channel

PDCP: Packet Data Convergence Protocol

PDN: Packet Data Network

PDSCH: Physical Downlink Shared Channel

PFCP:	Packet Forwarding Control Protocol
PGW:	PDN Gateway
PGW-C:	PGW Controller
PGW-U:	PGW User
PHICH:	Physical HARQ Indicator Channel
PHR:	Power HeadRoom
PMCH:	Physical Multicast Channel
PMI:	Precoder Matrix Indicator
PMIPv6:	Proxy Mobile IP version 6
PMK:	Pairwise Master Key
PPA:	Push-Profile-Answer
PPR:	Push-Profile-Request
PRACH:	Physical Random Access Channel
PRB:	Physical Resource Block
ProSe:	Proximity Service
PRS:	Positioning Reference Signal
PS:	Packet-Switched
PSBCH:	Physical Sidelink Broadcast Channel
PSCCH:	Physical Sidelink Control Channel
PSDCH:	Physical Sidelink Discovery Channel
PSM:	Power Saving Mode
PSPL:	Preferred Service Provider List
PSS:	Primary Synchronization Signal
PSSCH:	Physical Sidelink Shared Channel
PSSS:	Primary Sidelink Synchronization Signal
PTRS:	Phase Tracking Reference Signal
PUCCH:	Physical Uplink Control Channel
PUSCH:	Physical Uplink Shared Channel

Q

QAM:	Quadrature Amplitude Modulation
QCI:	QoS Class Identifier
QFI:	QoS Flow Identifier
QoS:	Quality of Service
QPP:	Quadratic Permutation Polynomial
QPSK:	Quadrature Phase-Shift Keying

R

RAA:	Re-Auth-Answer
RAR:	Re-Auth-Request
RAR:	Random Access Response
RB:	Resource Block
RDN:	Radio Distribution Network
RF:	Radio Frequency
RI:	Rank Indicator
RIA:	Reporting-Information-Answer
RIR:	Reporting-Information-Request
RLC:	Radio Link Control
RN:	Relay Node
RNTI:	Radio Network Temporary Identifier
ROHC:	Robust Header Compression
RP:	Resource Pool
RRC:	Radio Resource Control
RRH:	Remote Radio Head
RS:	Reference Signal
RSRP:	Reference Signal Received Power
RSRQ:	Reference Signal Received Quality

RSSI: Received Signal Strength Indication

RSU: Road Side Unit

RTA: Registration-Termination-Answer

RTP: Real-time Transport Protocol

RTR: Registration-Termination-Request

RU: Resource Unit

S

SA: Security Association

SA: Standalone

SAA: Server-Assignment-Answer

SAR: Server-Assignment-Request

SBCCH: Sidelink Broadcast Control Channel

SC: Sidelink Control

SCEF: Service Capability Exposure Function

SC-FDMA: Single-Carrier Frequency-Division Multiple Access

SCG: Secondary Cell Group

SCH: Sub-Channel

SCI: Sidelink Control Information

SCM: Single-Connection Mode

SC-PTM: Single-Cell Point-To-Multipoint

SCS: Services Capability Server

SCTP: Stream Control Transmission Protocol

SDAP: Service Data Adaptation Protocol

SDF: Service Data Flow

SDL: Supplementary Downlink

SDN: Software-Defined Networking

SDP: Session Description Protocol

SeGW: Security Gateway
SeNB: Secondary eNB
SFBC: Space Frequency Block Coding
SGW: Serving Gateway
SGW-C: SGW Controller
SGW-U: SGW User
SIA: Subscriber-Information-Answer
SIB: System Information Block
SIMO: Single Input Multiple Output
SIP: Session Initiation Protocol
SIR: Subscriber-Information-Request
SISO: Single Input Single Output
SL: Sidelink
SL-BCH: Sidelink Broadcast Channel
SL-DCH: Sidelink Discovery Channel
SLI: Sidelink Identifier
SL-MIB: Sidelink Master Information Block
SLP: SUPL Location Platform
SL-SCH: Sidelink Shared Channel
SLSS: Sidelink Synchronization Signal
SMS: Short Message Service
SMS-SC: SMS Service Center
SPR: Subscription Profile Repository
SR: Scheduling Request
SRB: Signaling Radio Bearer
SRS: Sounding Reference Signal
SSID: Service Set Identifier
SSS: Secondary Synchronization Signal

SSSS: Secondary Sidelink Synchronization Signal
STA: Session Termination Answer
STCH: Sidelink Traffic Channel
STR: Session Termination Request
SUL: Supplementary Uplink
SU-MIMO: Single-User MIMO
SUPL: Secure User Plane Location

T

TAI: Tracking Area Identity
TBCC: Tail-Biting Convolutional Coding
TC: Traffic Class
TDA: MT-Data-Answer
TDD: Time-Division Duplex
TDMA: Time-Division Multiple Access
TDR: MT-Data-Request
TEID: Tunnel Endpoint Identifier
TFT: Traffic Flow Template
TM: Transparent Mode
TMGI: Temporary Mobile Group Identity
TRP: Time Repetition Pattern
TSC: Transparent Single-Connection
TTI: Transmission Time Interval
TWAG: Trusted WLAN Access Gateway
TWAN: Trusted WLAN Access Network
TWAP: Trusted WLAN AAA Proxy

U

UCI:	Uplink Control Information
UE:	User Equipment
UICC:	Universal Integrated Circuit Card
UL:	Uplink
UM:	Unacknowledged Mode
U-NII:	Unlicensed National Information Infrastructure
UP:	User Plane
UpPTS:	Uplink Pilot Time Slot

V, W, X

V2I:	Vehicle to Infrastructure
V2N:	Vehicle to Network
V2P:	Vehicle to Pedestrian
V2V:	Vehicle to Vehicle
V2X:	Vehicle to everything
VoLTE:	Voice over LTE
WCDMA:	Wideband Code-Division Multiple Access
WFA:	Wi-Fi Alliance
Wi-Fi:	Wireless Fidelity
WLAN:	Wireless Local Area Network
WLANSP:	WLAN Selection Policy
WLCP:	WLAN Control Plane
XML:	Extensible Markup Language

Introduction

The era of cellular and digital telecommunications began in the 1990s with second-generation (2G) mobile networks, based on time-division multiple access (TDMA).

In the 2000s, third-generation (3G) networks were developed on the principle of wideband code-division multiple access (WCDMA). Although the third generation has dominated the market thanks to the increase in data throughput, it has never completely replaced the second generation.

The early 2010s saw the start of fourth-generation (4G) networks using orthogonal frequency-division multiple access (OFDMA) for the downlink and single-carrier frequency-division multiple access (SC-FDMA) for the uplink.

The development of 4G networks followed three steps identified by the releases of 3GPP (3rd Generation Partnership Project) standard:

– releases 8 and 9 are the basis of LTE (Long-Term Evolution) standard;

– releases 10, 11 and 12 are the basis of LTE Advanced standard;

– releases 13 and 14 are the basis of LTE Advanced Pro standard.

The 3GPP standardization body specified service models corresponding to specific use cases and requirements:

– MBB (Mobile Broadband) service corresponds to applications and services that require faster connection, which make it possible, for example, to watch videos in ultra-high definition or use virtual or augmented reality applications;

– LLC (Low Latency Communication) service groups together all the applications requiring extremely high reactivity as well as reliability of the data transmission service, for example civil security for critical missions;

– MTC (Machine Type Communication) service mainly groups applications linked to the Internet of Things (IoT). These services do not require very high bit rates, but require more extensive coverage and lower energy consumption.

I.1. LTE standard

Release 8 defines the evolved packet system (EPS) consisting of a new evolved packet core (EPC) coupled to a new evolved universal terrestrial radio access network (E-UTRAN).

Release 8 defines a new radio interface based on orthogonal frequency-division multiplexing (OFDM) and four-channel spatial multiplexing (MIMO (Multiple Input Multiple Output) 4×4). The MIMO function relies on the availability of the cell-specific reference signal (CRS).

Category-4 mobiles are able to achieve up to 150 Mbps for the downlink and up to 50 Mbps for the uplink, with the following characteristics for the radio interface:

– a radio channel bandwidth of 20 MHz;

– 64-QAM (Quadrature Amplitude Modulation) for the downlink and 16-QAM for the uplink;

– two-channel spatial multiplexing (MIMO 2×2) for the downlink.

LTE standard only offers services based on packet-switching (PS), and as such, only allows the transport of IP (Internet Protocol) packets. In release 9, the telephone service VoLTE (Voice over LTE) is therefore provided by the network IMS (IP Multimedia Sub-system). If the VoLTE is not deployed, the mechanism CSFB (Circuit-Switched Fallback) is used to redirect the mobile to 2G/3G networks in the CS mode in the case of an incoming or outgoing telephone call.

I.2. LTE Advanced standard

Release 10 provides throughput enhancement through carrier aggregation (CA), which increases the overall bandwidth of the radio channel.

The throughput improvement is also achieved by increasing the number of channels spatially multiplexed (MIMO 8×8). Additional resources are specifically allocated to each mobile for the channel state information reference signal (CSI-RS).

The modulation scheme has been increased from 64-QAM to 256-QAM, allowing an increase in the downlink bit rate.

Release 11 introduces new features to improve data throughput and edge coverage, with enhanced inter-cell interference coordination (eICIC) and coordinated multipoint (CoMP) transmission.

Release 12 defines a new MTC architecture that takes into account connected objects. A new category of mobile (category 0) is introduced, allowing a reduced energy consumption in return for a lower data rate.

LTE Advanced standard also defines the evolved Multimedia Broadcast/ Multicast Service (eMBMS) in order to broadcast content shared between multiple mobiles. In addition, in the areas of public safety and critical communications, the eMBMS network improves the efficiency of the MCPTT (Mission Critical Push-To-Talk) service that enables the transmission of voice to all participants of a group.

In addition, release 12 introduces proximity services, from device to device (D2D), to obtain a reduced latency for the time of both communication establishment and the voice transport.

I.3. LTE Advanced Pro standard

The goal of LTE Advanced Pro standard is to increase the throughput for mobiles to reach the value of Gigabit/s, to bring new functionalities to EPS, MTC and eMBMS networks, and to introduce new proximity services, namely vehicle to everything (V2X).

I.3.1. *MBB service*

I.3.1.1. *Network architecture*

The control and user plane separation (CUPS) aims to define a more flexible distributed architecture, taking advantage of the evolution towards software-defined networking (SDN) implementations.

The CUPS architecture is based on the separation between the user plane and the control plane for the serving gateway (SGW) and the PDN (Packet Data Network) gateway (PGW). This architecture enables mobile edge computing (MEC) deployments that leverage a distributed user plane, collocated with the evolved node base station (eNB), and a centralized control plane.

Dual connectivity (DC) introduced in release 12 improves the downlink throughput. IP packets are simultaneously transmitted from two eNB entities, the master eNB (MeNB) and the secondary eNB (SeNB).

Release 13 introduces the traffic transfer to two radio stations for the uplink, according to two parameters: a primary link and a threshold value. When the mobile buffer is below the threshold, the mobile only sends data on the primary link. When the amount of buffered data exceeds the threshold, the mobile can send data to both the MeNB and the SeNB.

I.3.1.2. *Spatial multiplexing*

A significant improvement in release 13 is the introduction of active antenna system (AAS), with antenna elements ranging from 8 to 64, which is relevant for frequencies above 3.5 GHz.

The FD-MIMO (Full-Dimension MIMO) mechanism enables beamforming in the horizontal and vertical directions and the generation of three-dimensional spatial links.

Associated with the FD-MIMO mechanism, two methods for using the CSI-RS are defined:

– for the method Class A, the CSI-RS is associated with an antenna element, their number being limited to 16;

– for the method Class B, the eNB entity can configure up to eight beams per mobile, each beam being formed from a CSI-RS.

Release 14 improves the FD-MIMO mechanism, for the method Class A, by increasing the number of CSI-RS up to 32 and decreasing the density of the CSI-RS. For the method Class B, the improvement concerns the efficiency of the CSI-RS.

I.3.1.3. *Channel aggregation*

Channel aggregation has increased to 32 (the number of aggregated components). In order to meet growing data traffic, LTE Advanced Pro standard has also introduced new aggregation techniques: LAA (License Assisted Access),

LWA (LTE–Wi-Fi Aggregation) and LWIP (LTE/WLAN radio level integration with IPsec tunnel).

LAA is an extension of LTE aggregation. Transmission is carried out on licensed (LTE) and unlicensed frequency bands (Wi-Fi at 5 GHz U-NII band), between the mobile and the eNB entity, without an intermediate access point. The eNB entity is the anchor point for channel aggregation.

LAA is similar to dual connectivity, for which LTE transmission takes place on the MeNB station and Wi-Fi transmission on the SeNB station.

In release 13, transmission on the unlicensed frequency band occurs only for the downlink. The transmission for the uplink exists in release 14.

LWA and LWIP use LTE and Wi-Fi frequency bands. The transmission on the Wi-Fi radio channel occurs between the mobile and the access point (AP) in accordance with the 802.11 standard. The eNB entity is the anchor point for channel aggregation.

Release 14 brings the following enhancements to the LWA features:

– transmission of data for the uplink on the Wi-Fi network;

– support for new 60 GHz frequency bands and 802.11a, 802.11ad and 802.11ay interfaces;

– collection of information for available capacity on the Wi-Fi network;

– discovery of neighboring Wi-Fi networks under the coverage of eNB entities.

LWIP uses an IPSec tunnel to transport IP packets between the eNB entity and the Wi-Fi access point. Unlike LWA, LWIP aggregation does not require any modification for Wi-Fi transmission.

I.3.2. *LLC service*

For D2D communication, the main improvement lies in the support of relaying by mobile. This allows, for public safety, mobiles out of coverage to communicate with the network via mobiles under the radio coverage.

The SC-PTM (Single-Cell Point-To-Multipoint) feature was introduced in release 13 to improve the efficiency of the radio interface of the eMBMS network, by supporting, on one cell, the broadcast service using specific radio resources.

Prior to release 13, the 3GPP organization standardized functionality for use as an enabler for mission-critical services. For example, an MCPTT group voice call must have a bearer already established for immediate use due to the time required to establish the bearer on the eMBMS network.

Release 13 defines different application services for the MCPTT function: user authentication, group affiliation, group calls and private calls, and floor control.

Release 14 completes the MCPTT function with various management services: configuration management, group management, identity management and key management.

Release 14 introduces vehicle-to-everything (V2X) communication, which comes in four applications depending on the different types of device to which the vehicle connects:

– vehicle-to-vehicle (V2V) communication;

– vehicle-to-infrastructure (V2I) communication;

– vehicle-to-pedestrian (V2P) communication;

– vehicle-to-network (V2N) communication.

I.3.3. *MTC service*

Release 13 changes the architecture of the network to optimize the data transfer using different planes:

– the control plane, to reduce the number of messages during the processing of a session establishment procedure;

– the user plane, for which the management of the connection avoids deleting the context when the terminal has no longer data to transmit.

The architecture enhancements for service capability exposure (AESE) is used to expose network services and capabilities to third parties, and to provide access to network capabilities:

– high latency communication, to support the scenario in which applications communicate with temporarily inaccessible terminals;

– point-to-multipoint communication;

– increase in the discontinuous reception (DRX) cycle;

– event monitoring affecting the terminal operation.

Terminals Cat. 1 and Cat. 0 were introduced in releases 8 and 12 respectively for MTC service. These terminals have reduced functionality but can operate in a bandwidth of 20 MHz.

To reduce the complexity of the terminal and improve the battery life and radio coverage, release 13 introduces two new technologies for the radio interface:

– LTE-M operating in a bandwidth of 1.4 MHz, with terminals Cat. M1;

– NB-IoT (NarrowBand Internet of Things) operating in a bandwidth of 180 kHz, with terminals Cat. NB1.

In order to increase the throughput on the radio interface, release 14 introduces two new categories of terminals: Cat. M2 for LTE-M and Cat. NB2 for NB-IoT.

I.4. Wi-Fi integration

Release 8 defines the integration of the Wi-Fi radio access network at the EPC, addressing all aspects of interworking: mobility between Wi-Fi and LTE access and security (authentication, protection of data). However, release 8 does not allow simultaneous connections to multiple access networks. In addition, release 8 specifies the access network discovery and selection function (ANDSF).

Several access architectures connected to the EPC are defined:

– the architecture based on the S2a interface, for which the Wi-Fi radio access network is trusted and the mobility is managed by the network;

– the architecture based on the S2b interface, for which the Wi-Fi radio access network is untrusted and the mobility is managed by the network;

– the architecture based on the S2c interface, for which the mobility is managed by the mobile and the Wi-Fi radio access network can be trusted or untrusted.

Release 9 improves the ANDSF feature that provides access network discovery and selection information for roaming scenarios.

Release 10 introduces simultaneous connections to several radio access technologies.

The NSWO (Non-Seamless WLAN Offload) feature allows traffic to be directly routed to the Internet network without crossing the EPC.

The MAPCON (Multi-Access PDN Connectivity) function supports various connections to the PDN transiting either via the LTE interface (e.g. telephone service) or via the Wi-Fi interface (e.g. Internet service), depending on the operator policy.

Release 12 improves the S2a solution using three modes of operation of offloading traffic:

– single-connection mode (SCM) supports the mobility between LTE and Wi-Fi access and NSWO via Wi-Fi access;

– multi-connection mode (MCM) supports one or more PDN connections and NSWO via Wi-Fi access at the same time;

– transparent single-connection (TSC) mode provides a single connection (LTE or Wi-Fi) and does not support the mobility between LTE and Wi-Fi access.

The discovery and selection functions are also defined in the 802.11u specification of the Institute of Electrical and Electronics Engineers (IEEE), integrated and supplemented by the Wi-Fi Alliance in the Hotspot 2.0 specification. Release 12 helped to align the ANDSF with Hotspot 2.0 features.

Release 13 completes the transfer modes for IP packets by introducing the IFOM (IP Flow Mobility) function for routing the different IP streams of a PDN connection, which corresponds to an access point name (APN), through both LTE and Wi-Fi interfaces.

I.5. 5G integration

The fifth generation (5G) of mobile networks, the first phase of which is defined in release 15, must be more flexible and scalable to allow a wider range of services. It will move to an architecture based on network function virtualization (NFV) where network elements are hosted in virtual environments, and network slicing allows adaptation to different requirements.

As in previous generations, the fifth generation defines a core network (5GC) and a radio access network (5G NR (new radio)). Unlike previous generations that required the deployment of the core and radio access network of the same generation, the fifth generation makes it possible to integrate elements of different generations in different configurations.

The 5G NR access network is defined to support two operational modes, namely standalone (SA) and non-standalone (NSA):

– in the NSA mode, the 5G NR connects to the 4G core network only for the user plane, the control plane being processed by the 4G radio access network;

– in the SA mode, the 5G NR connects to the 5G core network for the user plane and control plane data.

Although both of the operation modes should have coexisted from the beginning, a consensus has emerged to prioritize the NSA mode in order to quickly respond to the need for throughput. This mode exploits existing 4G deployments by combining LTE and NR radio resources with 4G network cores.

Release 15 does not provide a fundamental technological breakthrough on the 5G NR interface with respect to the 4G LTE radio interface, the multiple access mode being identical, but rather some adjustments with respect to time-division multiplexing structures, frequency-division multiplexing and error correction codes.

1

MBB Service – Network Architecture

1.1. Initial architecture

1.1.1. *Functional architecture*

The functional architecture of the EPS (Evolved Packet System) network is depicted in Figure 1.1, at the point when the mobile attaches to its home network.

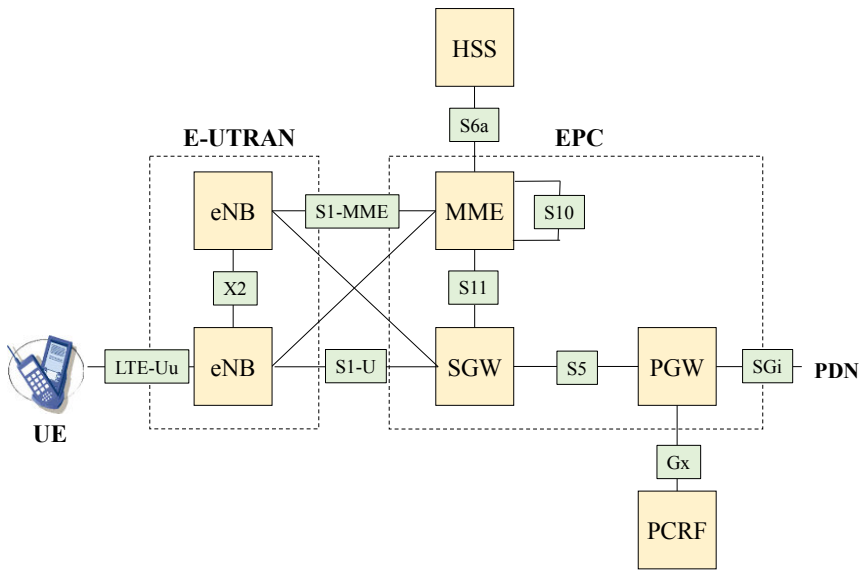

Figure 1.1. *Functional architecture of the EPS network*

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

The EPS mobile network consists of an EPC (Evolved Packet Core) network and an evolved universal terrestrial radio access network (E-UTRAN).

The E-UTRAN ensures the connection of the user equipment (UE), the resource allocation for the radio interface and the resource reservation when the mobile is switched from one cell to another.

The EPC interconnects the access networks, provides the interface to the packet data network (PDN) and controls the attachment of mobiles, the authorization to access the service and the establishment of bearers.

1.1.1.1. *eNB entity*

The E-UTRAN includes a single type of entity, the evolved node base station (eNB), which connects to the mobiles.

The eNB entity is responsible for the management of radio resources, for the control of the establishment of the data radio bearer (DRB), in which the mobile traffic is transmitted, and for its mobility management during the session (handover) which consists of a transfer of the DRB to another eNB entity.

This entity transfers the traffic data from the mobile (respectively from the SGW (Serving Gateway) entity) to the SGW entity (respectively to the mobile).

When the eNB entity receives data from the mobile or from the SGW entity, it refers to the QoS class identifier (QCI) for the implementation of the data scheduling mechanism.

The eNB entity can perform the marking of the DS (DiffServ) code point (DSCP) field of IP (Internet Protocol) header, based on the assigned QCI, for outgoing data to the SGW entity.

It performs compression and encryption of traffic data on the radio interface.

It performs encryption and integrity control of signaling data exchanged with the mobile.

It performs the selection of the mobility management entity (MME), part of the core network, to which the mobile is attached.

The eNB entity processes paging requests sent by the MME entity for their distribution in the cell corresponding to the radio coverage area of the eNB entity.

It also distributes system information of the cell, containing the technical characteristics of the radio interface and allowing the mobile to connect.

It uses the measurements made by the mobile to decide on the initiation of a cell change during a session (handover).

1.1.1.2. *MME entity*

The MME entity is the network control tower, allowing mobile access to the service and controlling bearer establishment for the transmission of traffic data.

The MME entities belong to a group (pool). Load balancing of the MME load is ensured by the eNB entities within a group that must have access to each MME entity of the same group.

The MME entity is responsible for attachment and detachment of the mobile.

During attachment, the MME entity retrieves the subscriber's profile and the subscriber's authentication data stored in the home subscriber server (HSS) and performs authentication of the mobile.

During attachment, the MME entity also registers the tracking area identity (TAI) of the mobile and allocates a globally unique temporary identity (GUTI) to the mobile which replaces the private international mobile subscriber identity (IMSI).

The MME entity manages a list of location areas (TAI) allocated to the mobile, within which the mobile in the idle state can move without contacting the MME entity to update its location area.

When attaching the mobile, the MME entity selects the SGW and PGW (PDN Gateway) entities for the construction of the default bearer, e.g. for the transport of IP packets containing SIP (Session Initiation Protocol) signaling or the data from Internet services.

For the construction of the bearer, the selection of the PGW entity is obtained from the access point name (APN) given by the mobile or by the HSS entity in the subscriber's profile.

The source MME entity also selects the target MME entity when the mobile changes both cell and group (pool).

The MME entity provides the information required for lawful interception, such as the mobile status (idle or connected), the location area if the mobile is idle or the E-UTRAN cell global identifier (ECGI) if the mobile is in session.

1.1.1.3. *SGW entity*

The SGW entities are also organized into groups (pools). To ensure load balancing of SGW load, each eNB entity within a group must have access to each SGW entity of the same group.

The SGW entity forwards incoming data from the PGW entity to the eNB entity and outgoing data from the eNB entity to the PGW entity.

When the SGW entity receives data from the eNB or PGW entities, it refers to the QCI for the implementation of the data scheduling mechanism.

For incoming data from the PGW entity, and outgoing data from the eNB entity, the SGW entity performs the DSCP field marking of the IP header of the S1 and S5 bearers, depending on the assigned QCI.

The SGW entity is the anchor point for the intra-system handover (mobility within the EPS network) provided that the mobile does not change group. Otherwise, the PGW entity performs this function.

The SGW entity is also the anchor point for the inter-system handover in the PS (Packet-Switched) mode, requiring the transfer of traffic data from the mobile to the second- or third-generation mobile network.

A mobile in the idle state remains attached to the MME entity. However, it is no longer connected to the eNB entity, and thus the radio bearer and the S1 bearer, built between the eNB and SGW entities, are deactivated.

The SGW entity informs the MME entity of incoming data when the mobile is in the idle state, which allows the MME entity to trigger the paging towards all eNB entities belonging to the same location area (TAI).

1.1.1.4. *PGW entity*

The PGW entity is the gateway router that provides the EPS network connection to the PDN (Internet network).

When the PGW entity receives data from the SGW entity or the PDN, it refers to the QCI for the implementation of the data scheduling mechanism.

The PGW entity can perform DSCP marking of the IP header of the S5 bearer, based on the assigned QCI.

During attachment, the PGW entity grants an IPv4 or IPv6 address to the mobile. If the assigned IPv4 address is a private address, the entity PGW performs network address and port translation (NAPT), in order to translate the IP addresses and the TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) port numbers.

The PGW entity constitutes the anchor point for inter-SGW mobility when the mobile changes groups.

It hosts the policy and charging enforcement function (PCEF) which allows the rules relating to mobile traffic data on packets, filtering, charging and quality of service (QoS) to be applied to the bearer to build.

The policy and charging rules function (PCRF), outside the EPS network, provides the PCEF of the PGW entity with the rules to apply when establishing bearers.

The PGW entity performs replication of the mobile traffic data within the framework of lawful interception.

1.1.1.5. *HSS entity*

The HSS entity is a database storing the data specific to each user. The main data stored include the identities of the users, the authentication parameters and the service profile.

When subscribing to the EPS network, the mobile is assigned a private identity (IMSI) which is associated with a service profile and a secret key (Ki).

The authentication parameters are used to control access to the mobile for attachment to the EPS network.

The service profile determines the services that the user has subscribed to.

1.1.1.6. *PCRF entity*

The PCRF entity provides to the PCEF entity, integrated in the PGW entity, the necessary information for the control and the charging of the traffic data (IP packets).

This information is stored in the subscription profile repository (SPR) during the creation of the subscription.

Traffic control includes the following:

– association between a service data flow (SDF) and the EPS bearer;

– blocking or allowing IP packets;

– assignment of the QCI parameter to the EPS bearer.

The PCEF entity executes the rules provided by the PCRF entity to control the traffic flow and the charging.

The PCEF entity may relate to the PCRF entity a change in state of a service flow, as in the case of loss of radio coverage of the mobile.

The PCRF entity may receive a session request from the application function (AF) as in the case of the establishment of a voice or conversational video communication initialized at the IP multimedia sub-system (IMS).

The PCRF entity may provide the AF entity with information about events occurring in the mobile network as in the case of loss of radio coverage of the mobile.

1.1.2. *Protocol architecture*

The protocol architecture of the EPS network is described in Figure 1.2 for the control plane and in Figure 1.3 for the user plane.

1.1.2.1. *LTE-Uu interface*

The LTE-Uu interface is the reference point between the mobile and the eNB entity (Figure 1.4).

This interface supports RRC (Radio Resource Control) signaling exchanged between the mobile and the eNB entity, transmitted in the signaling radio bearer (SRB) and the mobile traffic data (IP packets) transmitted in the data radio bearer (DRB).

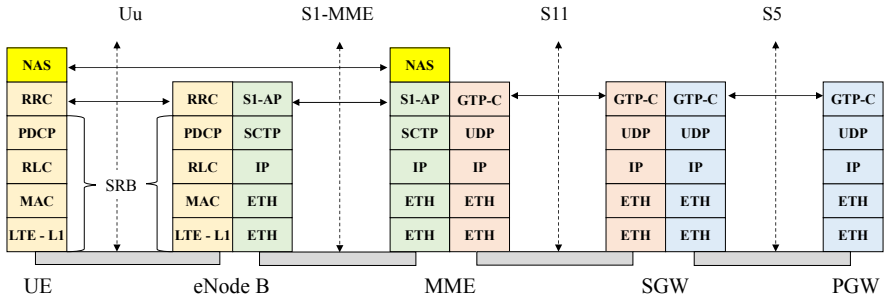

Figure 1.2. *Protocol architecture: the control plane*

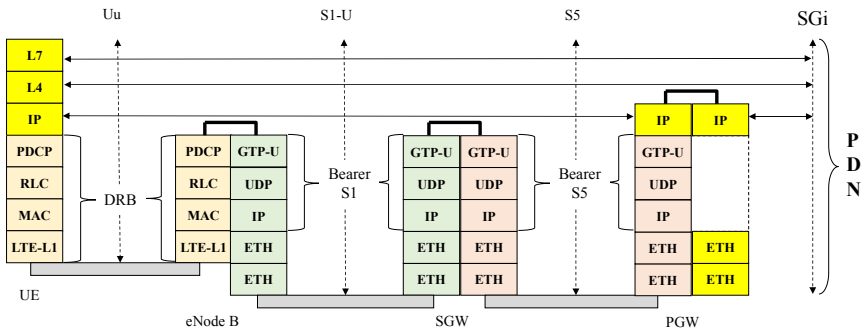

Figure 1.3. *Protocol architecture: the user plane*

The RRC protocol performs the following functions: broadcasting information system, control of the connection, control of the radio bearer, control of the handover and transfer of measurement reports.

RRC signaling also provides transport of the NAS (Non-Access Stratum) signaling messages exchanged between the mobile and the MME entity.

Traffic data corresponding to an IP packet and signaling data corresponding to an RRC message are encapsulated by the data link layer, which is divided into the following three sub-layers:

– PDCP (Packet Data Convergence Protocol);

– RLC (Radio Link Control);

– MAC (Medium Access Control).

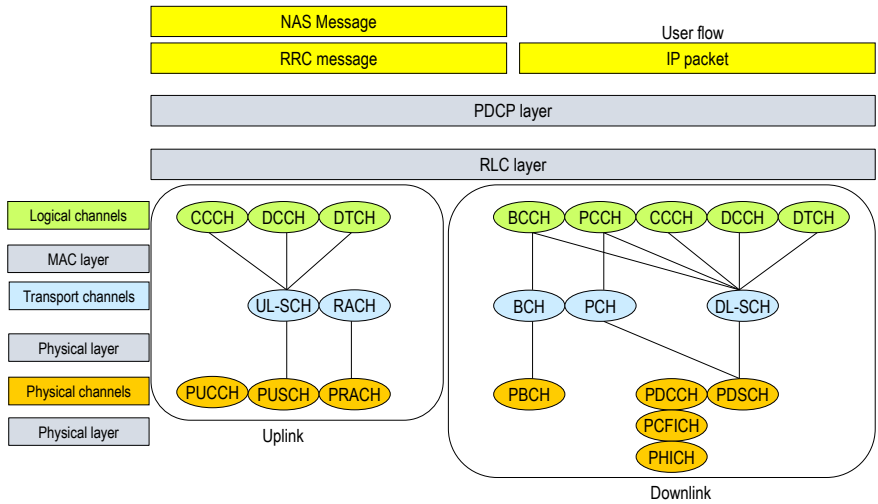

Figure 1.4. *Protocol architecture of the LTE-Uu interface*

The PDCP is used for RRC signaling messages related to dedicated control and for IP packets, and provides the following functions:

– compression of traffic data headers using the robust header compression (ROHC);

– security of traffic data (confidentiality) and RRC signaling (integrity and confidentiality);

– delivery in sequence of RRC messages and IP packets;

– recovery of PDCP frames lost during the handover.

The mobile can simultaneously activate multiple PDCP instances, each instance corresponding to a data radio bearer or a signaling radio bearer.

The RLC protocol provides control of the radio link between the mobile and the eNB entity.

The mobile can simultaneously activate multiple RLC instances, each instance corresponding to a PDCP instance.

The RLC protocol operates in three operation modes:

– acknowledged mode (AM);

– unacknowledged mode (UM);

– transparent mode (TM) for which no header is added to data.

The RLC protocol provides the following functions:

– retransmission in the case of error via the Automatic Repeat reQuest (ARQ) mechanism, for the acknowledged mode only;

– concatenation, segmentation and reassembly of PDCP frames in both the acknowledged and unacknowledged modes;

– possible re-segmentation of PDCP frames, in the acknowledgment mode, during a retransmission of the RLC frame;

– re-sequencing of received data in both the acknowledged and unacknowledged modes;

– detection of duplicate data in both the acknowledged and unacknowledged modes.

The MAC protocol provides the following functions:

– multiplexing RLC frames from multiple instances in a transport block;

– allocation of the radio resources via a scheduling mechanism for both transmission directions;

– management of retransmission in the case of error via the HARQ (Hybrid Automatic Repeat reQuest) mechanism;

– management of the random access procedure.

The physical layer consists of two subsets, whose interface constitutes the physical channel:

– for each transmission direction, the first subset comprises the error detection and correction codes and the rate adaptation;

– for the downlink, the second subset comprises the modulation, the spatial layer mapping, the precoding, the resource element mapping and the inverse fast Fourier transform (IFFT) for OFDM (Orthogonal Frequency-Division Multiplexing) signal generation (Figure 1.5);

– for the uplink, the second subset comprises the modulation, the mapping on the resource elements and the IFFT. The generation of the DFT-S-OFDM (Discrete Fourier Transform Spread OFDM) signal is obtained from a fast Fourier transform

(FFT). Spatial layer mapping and precoding are implemented only for the LTE Advanced interface (Figure 1.6).

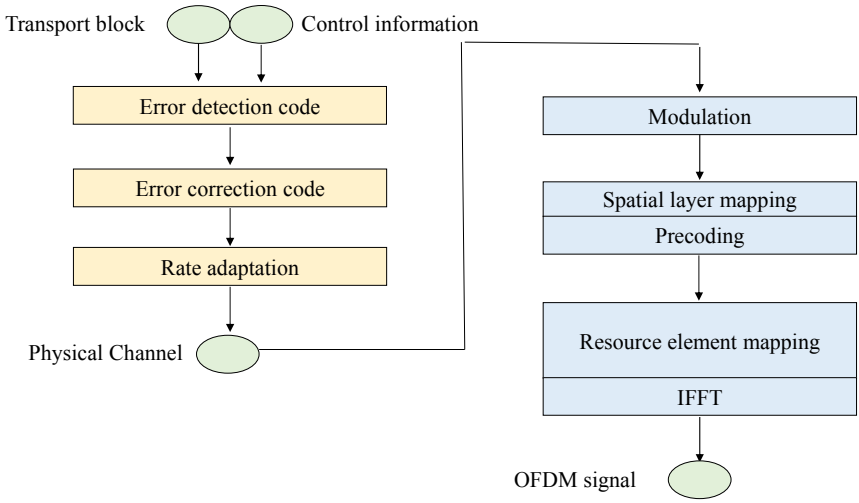

Figure 1.5. *The downlink chain of transmission*

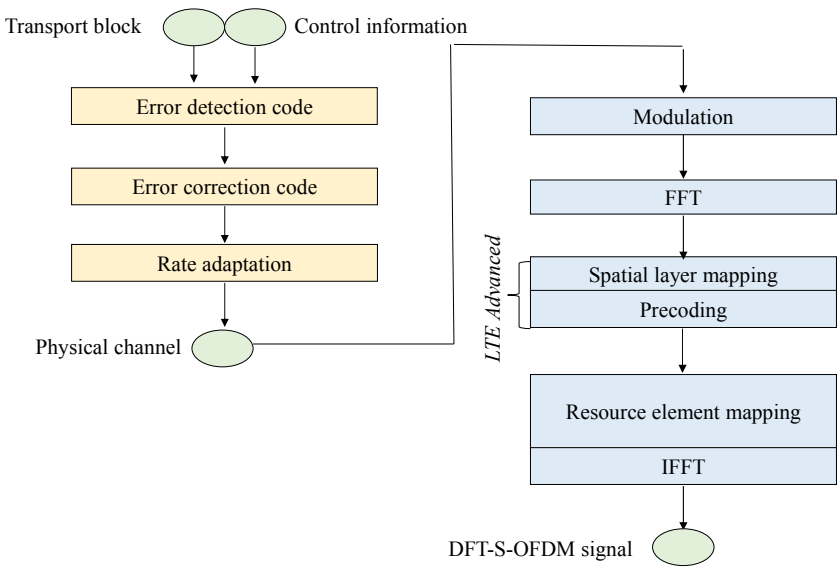

Figure 1.6. *The uplink chain of transmission*

1.1.2.2. *S1 interface*

The S1 interface is a group of interfaces between the E-UTRAN and the EPC, and consists of the S1-MME and S1-U interface.

The S1-MME interface is the reference point between the MME and eNB entities for signaling. This interface supports S1-AP (Application Part) signaling.

The S1-AP protocol provides the following functions: establishment of the mobile context; establishment, modification and release of the EPS radio access bearer (E-RAB), built between the mobile and the SGW entity; management of the handover; and paging.

The S1-AP protocol also provides the transport of the NAS signaling exchanged between the mobile and the MME.

The S1-U interface is a reference point between the eNB and SGW entities. This interface supports a GPRS tunneling protocol user (GTP-U), which encapsulates the IP packet flow.

1.1.2.3. *S11 interface*

The S11 interface is the reference point between the MME and SGW entities for signaling via the GPRS tunneling protocol control (GTPv2-C).

The GTPv2-C protocol supports the following functions: managing the context of the mobile and the S1 bearer and notification of incoming data when the mobile is in the idle state.

1.1.2.4. *S5 interface*

The S5 interface is the reference point between the SGW and PGW entities for signaling via the GTPv2-C protocol and traffic data (IP packets) via the GTP-U protocol.

1.1.2.5. *S10 interface*

The S10 interface is the reference point between MME entities. This interface is used when the mobile changes group (pool) and the MME must be relocated. It supports GTPv2-C signaling.

1.1.2.6. *SGi interface*

The SGi interface is the reference point between the PDW entity and the PDN (Internet).

1.1.2.7. *X2 interface*

The X2 interface is the reference point between two eNB entities. It is activated when both eNB entities belong to the same group.

This interface supports the X2-AP signaling for the control plane (Figure 1.7), and the GTP-U protocol for the IP packet flow when the mobile changes cell (Figure 1.8).

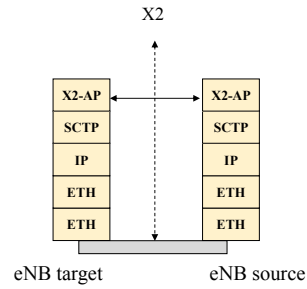

Figure 1.7. *Protocol architecture of the X2 interface: the control plane*

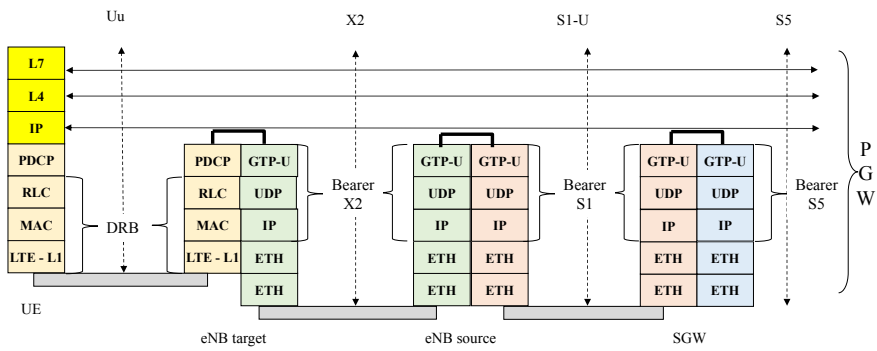

Figure 1.8. *Protocol architecture of the user plane during the handover based on the X2 interface*

The tunnel established between the two eNB entities is unidirectional (from the eNB source to the target eNB). It makes it possible to transfer to the target eNB entity the received traffic data from the SGW entity. It is temporarily established during the handover of the mobile.

1.1.2.8. *S6a interface*

The S6a interface is the reference point between MME and HSS entities. This interface supports DIAMETER signaling.

The DIAMETER protocol allows the MME to recover the authentication data and the service profile of the mobile.

1.1.2.9. *Gx interface*

The Gx interface is the reference point between the PCRF entity and the PCEF of the PGW entity. This interface supports DIAMETER signaling.

The DIAMETER protocol allows the PGW entity to recover rules applying to the EPS bearer and to inform the PCRF entity of the termination of the session on the EPS network.

1.2. CUPS architecture

The CUPS (Control and User Plane Separation) architecture consists of separating the functions of the control plane (CP) and user plane (UP) from the SGW and PGW entities.

This separation allows the flexibility of deployment of the EPC, the equipment that can be distributed or centralized, and an independent scaling between the functions of the CP and the UP.

The initial SGW entity is reconfigured from an SGW-U (User) entity, connecting S1 and S5 bearers, and an SGW-C (Control) entity, providing the control function of the SGW-U entity (Figure 1.9).

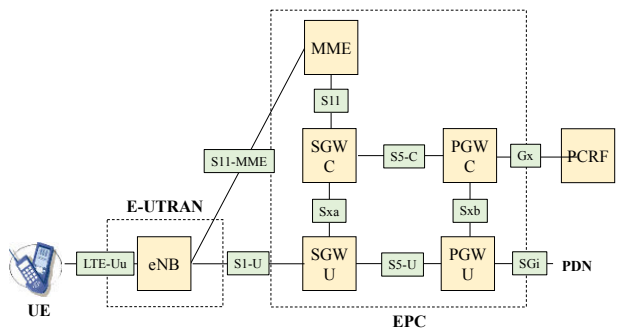

Figure 1.9. *CUPS architecture*

The initial PGW entity is reconfigured from a PGW-U entity, terminating the S5 bearer and routing the mobile flow, and a PGW-C entity, providing the control function for the PGW-U entity (Figure 1.9).

Latency can be reduced by selecting user plane nodes closer to the radio access network without increasing the number of control plane nodes.

Support for increased data traffic is achieved by adding nodes in the user plane without changing the number of SGW-C and PGW-C entities.

The Sxa interface (respectively Sxb) is the reference point between the SGW-C and SGW-U entities (respectively PGW-C and PGW-U). This interface supports PFCP (Packet Forwarding Control Protocol) signaling (Figure 1.10).

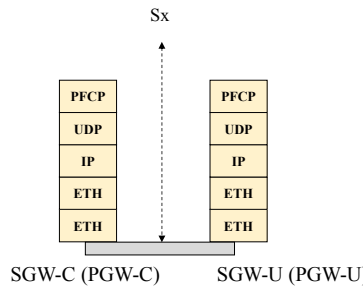

Figure 1.10. *Protocol architecture of the Sx interface: the control plane*

The CP and UP functions can evolve independently and implement the SDN (Software-Defined Networking) features providing centralized control and virtualization of functions.

A CP function can interface with several UP functions and a UP function can be controlled by several CP functions.

A mobile is served by a single SGW-C entity but several SGW-U entities can be selected for different PDN connections.

The CP function controls the processing of packets in the UP function by providing a set of rules in the Sx sessions:

– the rules relating to the packet detection rules for packet inspection;

– the rules relating to the transfer of packets;

– the rules relating to the control of the quality of service;

– the rules relating to the measurement of the traffic.

The S5-C interface is the reference point between the SGW-C and PGW-C entities. This interface supports GTPv2-C signaling.

The S5-U interface is the reference point between the SGW-U and PGW-U entities. This interface supports GTP-U tunneling of the IP packet of the stream.

The main features of the PFCP protocol are:

– an Sx association must be established between a CP function and a UP function before Sx sessions can be established on the UP function. The Sx association can be established by the CP function or by the UP function;

– an Sx session is established in the UP function to provide rules indicating the UP function how to handle certain traffic. An Sx session may correspond to a connection to the PDN or to a standalone session.

The procedures for the Sx association include the following:

– the establishment, modification and release of the Sx association;

– the checking that the remote PFCP application is active;

– the control to balance the load between the UP functions.

The procedures for the Sx session include the following:

– the establishment, modification and release of the Sx session;

– the Sx session report to signal specific events, for example reception of data, when the mobile is in the idle state.

Data transfer between the CP and UP functions is supported by GTP-U tunneling in order to transmit user plane data to the SGW-C (see network optimization described in section 10.2).

1.3. Heterogeneous networks

The E-UTRAN is homogeneous when coverage is done from macro cells.

The coverage of macro cells can vary from a kilometer to a few tens of kilometers. The output power is of the order of tens of watts.

One way to extend a radio access network in order to increase the traffic flow capacity, while maintaining it as a homogeneous network, is to densify it by adding more sectors per eNB entity or to decrease the size of the macro cell to constitute micro cells.

Micro cells usually cover smaller areas of up to one kilometer. They typically transmit in a power range of a few milliwatts to a few watts.

However, the reduction in the size of the cell has limits because finding new sites becomes increasingly difficult and expensive, especially in the city centers.

An alternative to extending a radio access network deployed from macro cells is to introduce small cells by adding existing low-power radio stations or remote radio heads to existing macro cells. The acquisition of the site is easier and less expensive with this type of equipment.

The HeNB (Home eNB) radio station is used to build femto cells and to provide additional coverage inside buildings.

The relay node (RN) is another type of low-power radio station. The relay node is connected to a DeNB (Donor eNB) radio station via an LTE-Uu-type radio interface. From the perspective of the mobile, the relay node acts as an eNB entity. From the perspective of the DeNB entity, the relay node acts as a mobile.

The remote radio head (RRH), connected to an eNB entity via an optical fiber, can also be used to provide a small cell coverage, the assembly constituting a distributed radio station.

Dual connectivity (DC) allows simultaneous connections on a macro cell and a small cell to improve traffic flow capacity. The aggregation of the radio resources of the two cell types is performed by the eNB entity of the macro cell.

1.3.1. *HeNB station*

The first architecture variant of the E-UTRAN implementing the HeNB entity is described in Figure 1.11.

This variant is similar to the initial architecture:

– the HeNb and MME entities are the terminations of the S1-MME interface;

– the HeNB and SGW entities are the terminations of the S1-U interface.

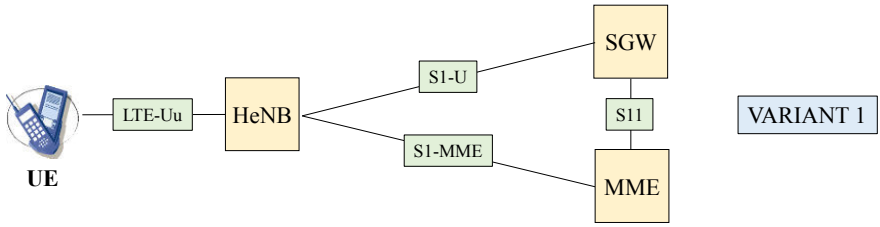

Figure 1.11. *Functional architecture implementing the HeNB station: variant 1*

This variant has the following drawbacks:

– an SCTP (Stream Control Transmission Protocol) association is set up between each HeNB entity and the MME entity. The messages of the presence control of the association ends (heartbeat) can create an overhead on the MME entity;

– the user can turn the HeNB entity on and off. Frequent establishment and release messages from the SCTP association may also create an overhead on the MME entity;

– a GTP-U tunnel is connected between each HeNB entity and the SGW entity. The control messages associated with the GTP-U tunnel (Path, Echo) can also create an overhead at the SGW entity.

The second architecture variant of the E-UTRAN implementing the HeNB entity is described in Figure 1.12. This variant introduces a new HeNB GW (Gateway) entity between, on the one hand, the HeNB entity and, on the other hand, the MME and SGW entities.

The HeNB GW entity concentrates the SCTP associations with each HeNB entity and creates a single SCTP association with the MME entity. This arrangement makes it possible to reduce the load of the MME entity.

The HeNB GW entity makes a connection between the media created, on the one hand, between each HeNB entity and the HeNB GW entity and, on the other hand, between the HeNB entity and the SGW entity. This arrangement makes it possible to limit, at the SGW entity level, the number of control messages associated with the GTP-U tunnel.

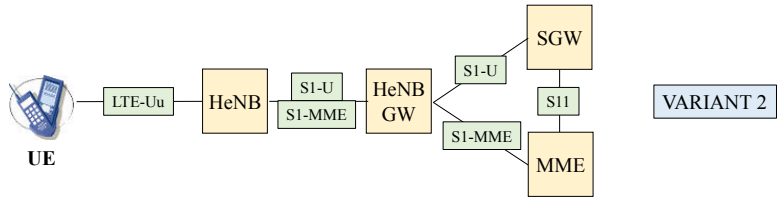

Figure 1.12. *Functional architecture implementing the HeNB station: variant 2*

The third architecture variant of the E-UTRAN implementing the HeNB entity is described in Figure 1.13. This variant introduces the HeNB GW entity only between each HeNB entity and the MME entity, which limits the load only for the MME entity.

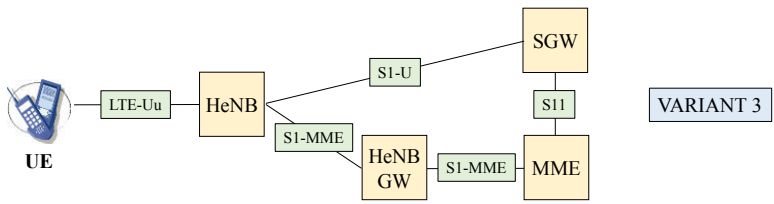

Figure 1.13. *Functional architecture implementing the HeNB station: variant 3*

The HeNB entity can operate in one of the following three different access modes:

– closed access: the HeNB entity is associated with a closed subscriber group (CSG) whose access is allowed. Closed access is applicable to residential deployment;

– open access: the HeNB entity is open to all of the operator's customers. Open access is applicable to deployment in high traffic areas, such as railway stations and airports;

– hybrid access: as for closed access, the HeNB entity is reserved for a group of users, but it is also accessible to the operator's customers, with a lower priority level.

In order to limit the number of SCTP associations that the HeNB entity has to establish with its neighbors on the X2 interface, an X2-GW concentrator can be integrated into the HeNB GW entity. A single SCTP association is established between the X2-GW concentrator and each HeNB entity.

Table 1.1 summarizes the handover possibilities between the HeNB and eNB entities depending on the type of access.

Source	Target
eNB or HeNB (any type of access)	HeNB with open access
eNB or HeNB (any type of access)	HeNB with hybrid access
HeNB with hybrid or closed access	HeNB with closed access (1)
HeNB (any type of access)	eNB

(1) Only for a closed subscriber group.

Table 1.1. *Different types of X2-based handover*

1.3.2. *Relay node*

The architecture of the E-UTRAN implementing the relay node (RN) is described in Figure 1.14.

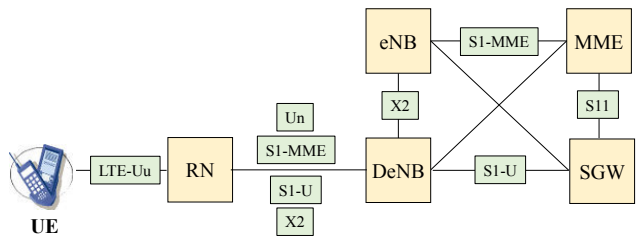

Figure 1.14. *Functional architecture implementing the relay node*

The frequency bands used by the relay node may be different for the LTE-Uu and Un interfaces or the same if the coverage areas of the RN and DeNB entities are disjoint.

A time division of the frame between the LTE-Uu and Un interfaces is necessary to use the same frequency band for these two interfaces while having a coverage area common to both RN and DeNB entities.

Since the relay node (RN) is considered as a mobile by the DeNB entity, it exchanges NAS messages with the MME entity, carried by the following protocols (Figure 1.15):

– RRC, exchanged between the relay node and the DeNB entity, via the Un interface;

– S1-AP, exchanged between the DeNB and MME entities, via the S1-MME interface.

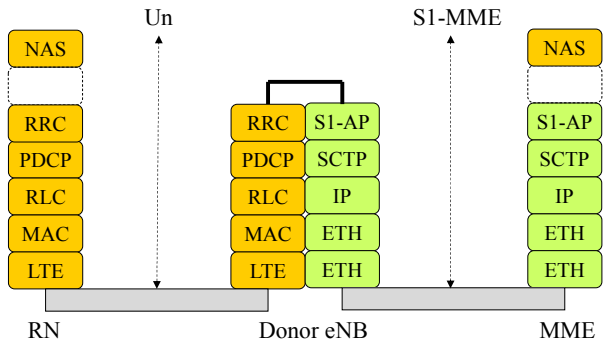

Figure 1.15. *Connecting the relay node: the control plane*

The DeNB entity acts as a proxy for S1-AP messages exchanged between the relay node and the MME entity (Figure 1.16) and for X2-AP messages exchanged between the relay node (respectively source or target) and the eNB entity (respectively target or source).

NAS messages exchanged between the mobile and the MME entity are carried by the following messages (Figure 1.16):

– RRC, exchanged between the mobile and the relay node, via the LTE-Uu interface;

– S1-AP, exchanged between the relay node and the DeNB entity, via the S1-MME interface;

– S1-AP, exchanged between the DeNB and MME entities, via the S1-MME interface.

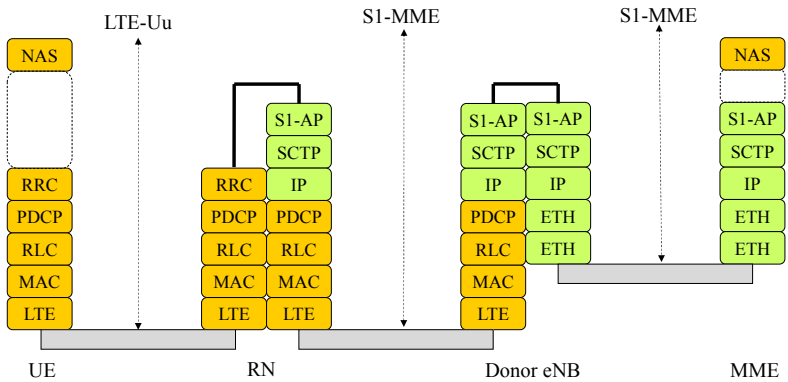

Figure 1.16. *Connecting the mobile: the control plane*

The mobile stream (IP packet) is transmitted in bearers to the SGW entity (Figure 1.17):

– the data radio bearer (DRB), on the LTE-Uu interface;

– the GTP-U tunnel, built between the relay node and the DeNB entity, on the S1-U interface;

– the GTP-U tunnel, built between the DeNB and SGW entities, on the S1-U interface.

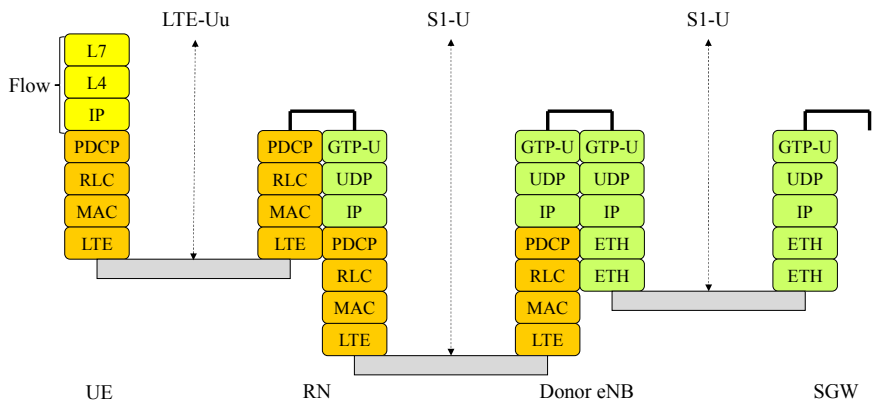

Figure 1.17. *Connecting the mobile: the user plane*

The DeNB entity provides the connection of established bearers, on the one hand, between the relay node and the DeNB entity and, on the other hand, between the DeNB and SGW entities.

The X2 interface is the reference point, on the one hand, between the eNB and DeNB entities and, on the other hand, between the DeNB entity and the relay node.

The X2 interface supports X2-AP signaling for the control plane (Figure 1.18), and GTP-U tunneling for the IP packet of the flow, when the mobile changes cell during the session (Figure 1.19).

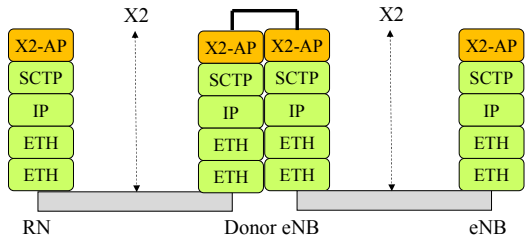

Figure 1.18. *Protocol architecture of the X2 interface: the control plane*

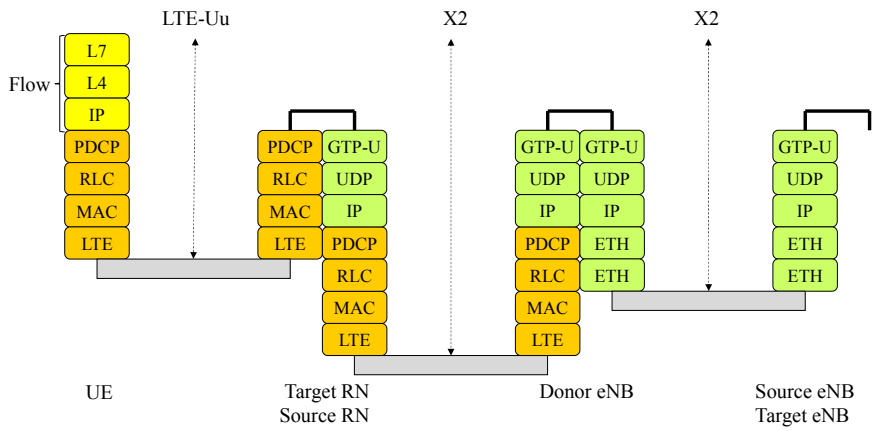

Figure 1.19. *Protocol architecture of the X2 interface: the user plane*

The DeNB entity provides unidirectional tunnels for the following media: source eNB entity to target RN entity or source RN to target eNB.

These tunnels transfer the user data received from the SGW entity to the target eNB entity or the target RN entity. It is temporarily established during the handover of the mobile.

1.3.3. *RRH module*

The eNB entity consists of two modules: the base band unit (BBU) providing the various processing and the radio transmitters/receivers. The remote radio head (RRH) is obtained from a removal of the transmitters/receivers via an optical fiber (Figure 1.20).

C-RAN (Cloud Radio Access Network) makes it possible to benefit from decentralized radio equipment that is simpler, easier and less expensive to maintain. In addition, the centralization and the virtualization of the BBU module make it possible to share its use for several cells.

The common public radio interface (CPRI) defines the communication between the BBU and RRH modules.

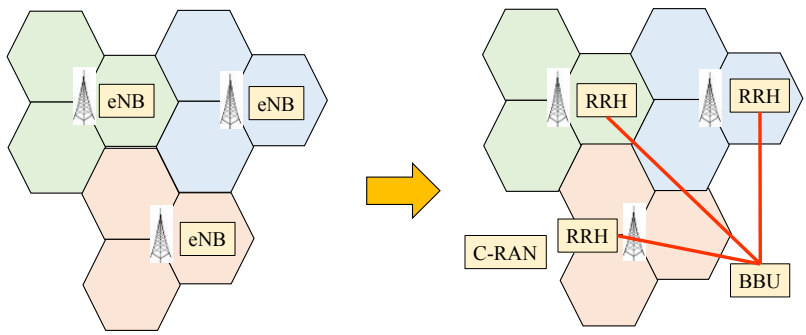

Figure 1.20. *C-RAN architecture*

Tables 1.2 and 1.3 provide the characteristics of the CPRI rate in the case of a 20 MHz radio channel for one antenna.

Sampling frequency	30.72 MHz
Number of bits per sample	30
CPRI payload rate	921.6 Mbps

Table 1.2. *CPRI payload rate*

Number of bits for the CPRI payload	240
Number of bits for the CPRI header	16
CPRI payload rate	921.6 Mbps
CPRI frame rate	983 Mbps
CPRI rate (8B/10B)	1.2288 Gbps

Table 1.3. *CPRI rate*

All operations above the physical layer and most of those in the physical layer are performed by the BBU module, which generates the radio signal, samples it and sends the resulting data to the RRH module.

The RRH module reconstructs the waveform and transmits it over the radio interface. The case of the uplink is similar, although the sampling of the radio signal must be done in the RRH module.

Figure 1.21 shows the functional distribution between the BBU and RRH modules for the downstream direction.

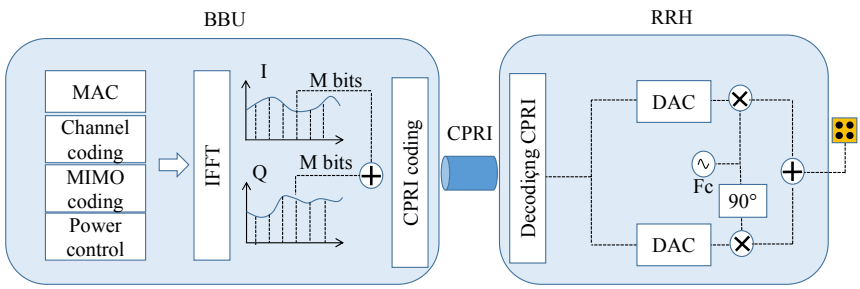

Figure 1.21. *Distribution of functions between the BBU and RRH modules*

The basic CPRI module (option 1) has a data rate of 614.4 Mbps. A 20 MHz radio channel uses two basic CPRI modules (option 2). A 20 MHz radio channel using the 2 × 2 MIMO (Multiple Input Multiple Output) transmission mode consumes four basic CPRI modules (option 3), a bit rate of 2.4576 Gbps.

The number of radio channels carried on the CPRI for an antenna depends on the rate of the radio interface and the bandwidth of the radio channel (Table 1.4).

CPRI rate (option) (Mbps)		Coding	Radio channel bandwidth		
			10 MHz	15 MHz	20 MHz
			Radio channel rate (Mbps)		
			614.4	92116	1228.8
Option 1	614.4	8B/10B	1	0	0
Option 2	1228.8	8B/10B	2	1	1
Option 3	2457.6	8B/10B	4	2	2
Option 4	3072	8B/10B	5	3	2
Option 5	4915.2	8B/10B	8	5	4
Option 6	6144	8B/10B	10	6	5
Option 7	9830.4	8B/10B	16	10	8
Option 8	10137.6	64B/66B	20	13	10
Option 9	12165.12	64B/66B	24	16	12

Table 1.4. *Number of radio channels carried on the CPRI*

1.3.4. *Dual connectivity*

Dual connectivity (DC) is a mechanism for sharing the transmission of IP packets between two radio stations: the master eNB station (MeNB), which covers a macro cell, and the secondary eNB station (SeNB), which usually covers a small cell (Figure 1.22).

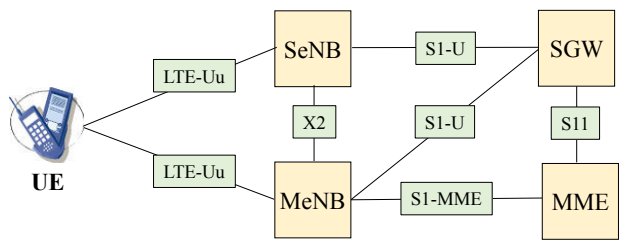

Figure 1.22. *Functional architecture implementing dual connectivity*

1.3.4.1. *User plane*

Two types of architecture are defined for the user plane (Figure 1.23):

– for the 3C architecture, the GTP-U tunnels of the S1-U interface, corresponding to the master cell group (MCG), terminate at the MeNB entity and some bearers (split bearers) are transferred from the MeNB entity to the SeNB entity, in GTP-U tunnels, on the X2 interface, at the PDCP layer;

– for the 1A architecture, the GTP-U tunnels of the S1-U interface, corresponding to the MCG, terminate at the MeNB entity, and those corresponding to the SCG at the SeNB entity level.

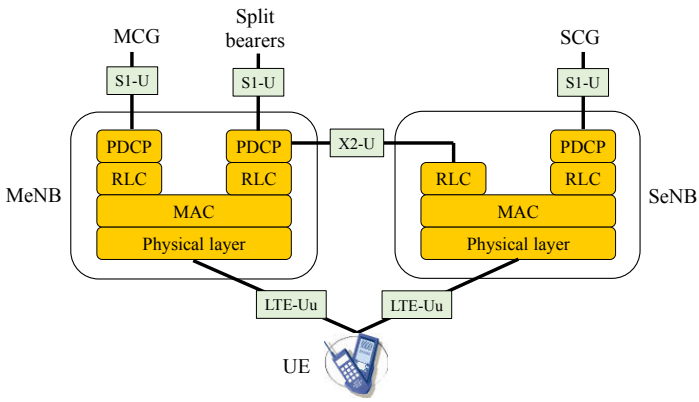

Figure 1.23. *Protocol architecture of the radio interface implementing dual connectivity*

1.3.4.2. *Control plane*

RRC messages are exchanged only between the mobile and the MeNB entity, on the LTE-Uu interface.

S1-AP messages are exchanged only between the MeNB and MME entities, on the S1-MME interface.

NAS messages exchanged between the mobile and the MME entity are carried by the RRC messages on the LTE-Uu interface and the S1-AP messages on the S1-MME interface.

X2-AP messages exchanged between the MeNB and SeNB entities must be enriched to account for dual connectivity:

– creating, modifying and terminating the context at the SeNB entity level;

– the transmission of the PDCP frame on the X2 interface and the management of the sequence numbers of the frame (3C architecture);

– the handover management, taking into account the change of SeNB entities, while maintaining the MeNB entity, the downstream data to be transferred from the source SeNB entity to the MeNB entity (1A architecture);

– the handover management, taking into account the change of MeNB entities, the downstream data to be transferred from the SeNB entity to the source MeNB entity (1A and 3C architectures).

2

MBB Service – Spatial Multiplexing

2.1. Multiplexing techniques

2.1.1. *MIMO mechanism*

The term SU-MIMO (Single-User Multiple Input Multiple Output) refers to a transmission to the same mobile, using the same frequency and time resource, on two antennas (MIMO 2 × 2) (Figure 2.1), four antennas (MIMO 4 × 4) or eight antennas (MIMO 8 × 8).

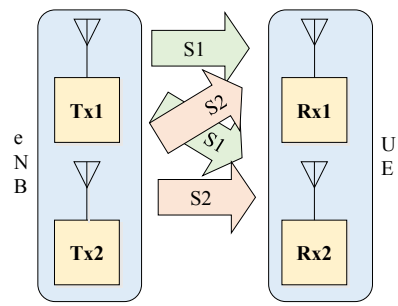

Figure 2.1. *SU-MIMO mechanism*

The term MU-MIMO (Multi-User MIMO) refers to a transmission to different mobiles, using the same frequency and time resource, on two antennas (MIMO 2 × 2) (Figure 2.2), four antennas (MIMO 4 × 4) or eight antennas (MIMO 8 × 8).

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

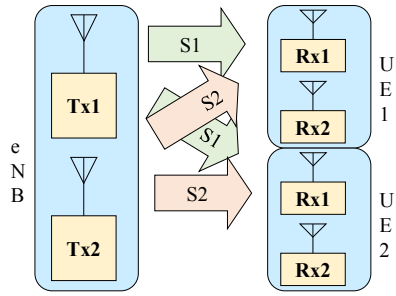

Figure 2.2. *MU-MIMO mechanism*

The MIMO mechanism improves the radio interface data rate thanks to the spatial multiplexing transmission of different signals emitted by the different antennas, each transmission sharing the same frequency and time resource.

The signal x1 (respectively x2) is transmitted by the transmitter Tx1 (respectively Tx2). The signal y1 (respectively y2) is received by the receiver Rx1 (respectively Rx2). The transmission matrix H contains the transfer functions hij, from the transmitter j to the receiver i.

On the reception side, the received signals y1 and y2 are the product of the transmitted signals x1 and x2 by the transmission matrix H.

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} h_{11} h_{12} \\ h_{21} h_{22} \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

The spatial demultiplexing consists of recovering the components x1 and x2 from the received signals y1 and y2 and the knowledge of the transmission matrix H.

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} h_{11} h_{12} \\ h_{21} h_{22} \end{bmatrix}^{-1} \times \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

The inverse matrix is estimated using two methods: minimum mean square error (MMSE) or zero forcing (ZF).

2.1.2. *Beamforming*

Beamforming is a complementary mechanism of MIMO. The beamforming technique uses multiple antennas to control the beam direction by individually weighting the amplitude and phase of each transmitted signal, by applying a specific precoding matrix to each component of the transmitted signal (Figure 2.3).

The precoding matrix can be determined by the mobile using the direction of arrivals (DoA). This technique is based on the analysis of the spectrum (the main lobe and the secondary lobes) of the received signal whose peaks identify the arrival angles.

Using beamforming, it is possible to logically reduce the beam opening angle and to limit the level of interference between the cells.

Using beamforming, it is also possible to increase the range thanks to the gain of power due to the contribution of each emitted signal.

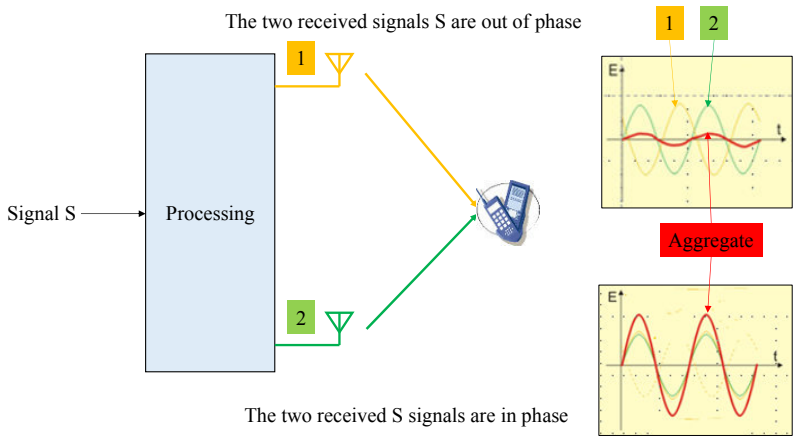

Figure 2.3. *Beamforming*

2.1.3. *Antenna configurations*

The transmission modes implementing beamforming and MU-MIMO require a good correlation between the antennas.

The transmission modes implementing transmission diversity and SU-MIMO require a decorrelation between the antennas.

For an antenna made of columns of radiating components with vertical polarization, the correlation between the columns is relatively strong.

For an antenna made of a column of two sets of radiating components, each set corresponding to a crossed polarization ± 45 degrees, the correlation is relatively weak.

The antenna configurations are described in Figure 2.4 and relate to a single frequency band.

Configuration A corresponds to an antenna made of a column of radiating components with vertical polarization.

Configuration B corresponds to an antenna made of a dual column of radiating components with vertical polarization.

Configuration C corresponds to an antenna made of four columns of radiating components with vertical polarization.

Configuration D corresponds to an antenna made of a column of two sets of radiating components, each set corresponding to a crossed polarization ± 45 degrees.

Configuration E corresponds to an antenna made of two columns, each column comprising two radiating component sets, each set corresponding to a crossed polarization ± 45 degrees.

Configuration E combines pairs of correlated radiating components of the same polarization, and pairs of decorrelated radiating components with different polarization.

Configuration F corresponds to an antenna made with:

– a central column of two sets of radiating components, each set corresponding to a crossed polarization ± 45 degrees;

– two separate sets, each set comprising radiating components, corresponding to one of the two crossed polarizations ± 45 degrees.

The remaining polarization remains available for use in another frequency band.

Configuration G corresponds to an antenna made of four columns of radiating components, each column comprising two sets of radiating components, each set corresponding to a crossed polarization ± 45 degrees.

Configuration H corresponds to two separate antennas, each antenna being made of a column of two sets of radiating components, each set corresponding to a crossed polarization ± 45 degrees.

Configuration I corresponds to two separate antennas, each antenna being made of a column of radiating components with vertical polarization.

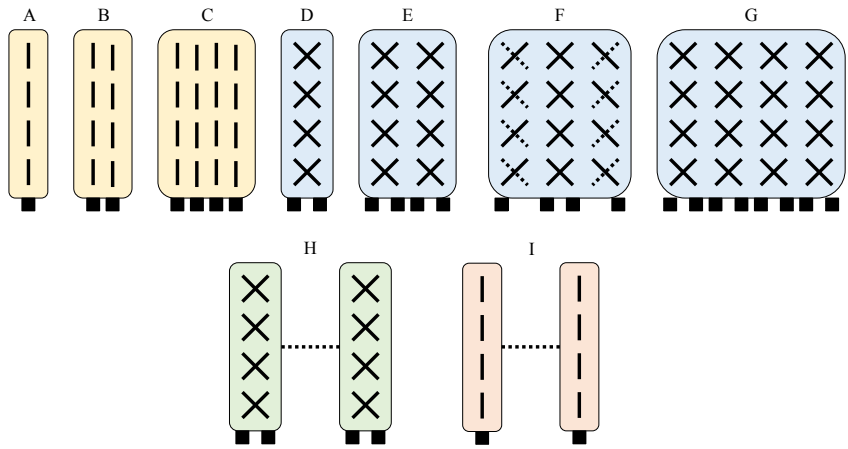

Figure 2.4. *Antenna configurations*

2.2. Antenna ports

2.2.1. *Downlink*

The symbols produced by the modulation are distributed over spatial layers, and then precoded.

The precoded symbols are associated with the reference signal (RS) to form antenna ports.

Table 2.1 shows the association of the antenna ports and the reference signals for the downlink.

Each of the antenna ports p0 to p3 is associated with a physical antenna.

The antenna port p4 is associated with a single physical antenna.

The antenna port p5 is associated with two or four physical antennas.

The antenna port p6 is associated with a single physical antenna.

Each of the antenna ports p7 to p14 and p15 to p22 is associated with a physical antenna.

Antenna ports	Reference signal
p0 to p3	CRS
p4	MBSFN-RS
p5	UE-specific RS
p6	PRS
p7 and p8	UE-specific RS
p9 to p14	UE-specific RS
p15 to p22	CSI-RS

Table 2.1. *Association of the antenna ports and reference signals: downlink*

2.2.1.1. *CRS*

The cell-specific reference signal (CRS) is used to perform coherent demodulation of the received signal.

The coherent demodulation of the received signal is based on the calculation of the transfer function of the radio channel.

The CRS allows the implementation of spatial multiplexing and transmission diversity.

The CRS makes it possible to measure the reference signal received power (RSRP) and the reference signal received quality (RSRQ).

The CRS is transmitted in each sub-frame and covers the entire bandwidth of the radio channel.

2.2.1.2. *MBSFN-RS*

The MBMS single frequency network reference signal (MBSFN-RS) is only transmitted in the physical multicast channel (PMCH) for coherent demodulation of the received signal.

The PMCH is used to transmit IP (Internet Protocol) packets in the broadcast mode.

2.2.1.3. *UE-specific RS*

The UE-specific reference signal is used for the beamforming mechanism and for the spatial multiplexing of multiple users, and allows the demodulation of the physical downlink shared channel (PDSCH).

The UE-specific RS allows the following configurations:

– one user using a single spatial layer;

– one user using two spatial layers, and a beamforming associated with MIMO 2×2;

– two users using two spatial layers, the multiplexing of the two users being carried out by an identity code;

– four users using a spatial layer, the multiplexing of the four spatial layers being obtained from an orthogonal covering code (OCC) and an identity code;

– one user using eight spatial layers, and a beamforming associated with the MIMO 8×8.

2.2.1.4. *PRS*

The positioning reference signal (PRS) is used by the mobile to implement the observed time difference of arrival (OTDOA).

The OTDOA function is based on the measurement by the mobile of the difference in the time of reception of the PRS with respect to a reference cell.

The location of the mobile is obtained from three measurements made on three geographically dispersed cells.

2.2.1.5. *CSI-RS*

The channel state information reference signal (CSI-RS) improves the measurement of the received signal and the level of interference compared to that provided from the CRS-RS.

The power of the CSI-RS is either transmitted to determine the level of the received signal or suppressed to measure the level of interference.

2.2.2. *Uplink*

Table 2.2 shows the association of the antenna ports and the physical channels or signals for the uplink.

The number of the antenna port depends on the number of antenna ports identified by the index $\tilde{p}$.

Physical channel or signal	Index $\tilde{p}$	Antenna ports		
		1 port	2 ports	4 ports
PUSCH SRS	0	10	20	40
	1	–	21	41
	2	–	–	42
	3	–	–	43
PUCCH	0	100	200	–
	1	–	201	–

Table 2.2. *Numbering of antenna ports for the uplink*

Antenna ports 10 and 100 use a single physical antenna $\tilde{p} = 0$.

Antenna ports 20 and 200 (21 and 201 respectively) use the physical antenna $\tilde{p} = 0$ ($\tilde{p} = 1$ respectively).

Each of the antenna ports 40 to 43 uses a physical antenna.

2.3. UCI

The uplink control information (UCI) is information transmitted by the mobile and contains the scheduling request (SR), the HARQ indicator (HI) and the CSI.

The HI relates the positive (ACK) or negative (NACK) acknowledgment of data received on the PDSCH.

The CSI, estimated by the mobile, regroups the information related to the status report of the signal received on the PDSCH:

– the channel quality indicator (CQI) represents the modulation and coding scheme recommended for the PDSCH;

– the rank indicator (RI) determines the number of spatial layers recommended for the PDSCH;

– the precoder matrix indicator (PMI) provides indications related to the precoding matrix in the case of using spatial multiplexing, in closed loop, or in the case of beamforming.

The report of the CSI can be periodic or aperiodic.

The aperiodic report is always transferred in the physical uplink shared channel (PUSCH).

The periodic report is transferred in the physical uplink control channel (PUCCH) in the two following cases:

– no resource is allocated to the mobile in the PUSCH;

– a resource is allocated to the mobile and the simultaneous transmission of the PUCCH and PUSCH is possible.

Otherwise, the periodic report is transmitted in the PUSCH.

The report transfer modes are built based on the return type of CQI and PMI.

The type of transfer of the aperiodic or periodic report is communicated to the mobile by the RRC (Radio Resource Control) messages: *ConnectionSetup*, *ConnectionReconfiguration* or *ConnectionReconfiguration*.

The aperiodic report allows feedback related to the CSI in relation to the totality or to a part of the bandwidth of the radio channel defined by the mobile or the eNB entity (Table 2.3).

The transfer of the aperiodic report is triggered by the following messages:

– the downlink control information (DCI) transmitted in the physical downlink control channel (PDCCH);

– the random access response (RAR) transmitted in the PDSCH.

The periodic report allows feedback to the CSI in relation to the totality or to a part of the bandwidth of the radio channel defined only by the eNB entity (Table 2.4).

		Return PMI		
		No PMI	**Single PMI**	**Multiple PMI**
CQI return	**Wide band**			Mode 1-2
	Sub-band per UE	Mode 2-0		Mode 2-2
	Sub-band per eNB	Mode 3-0	Mode 3-1	

Table 2.3. *Transfer modes of the aperiodic reports*

		Return PMI	
		No PMI	**Single PMI**
CQI return	**Wide band**	Mode 1-0	Mode 1-1
	Sub-band per eNB	Mode 2-0	Mode 2-1

Table 2.4. *Transfer modes of the periodic reports*

2.4. Transmission modes

2.4.1. *Downlink*

Transmission mode 1 (TM1) is the SISO (Single Input Single Output) type. It corresponds to setting a transmitter to the antenna port p0. When the mobile is equipped with two receptors, it can implement the reception diversity.

Transmission mode 2 (TM2) is specified for MISO (Multiple Input Single Output). It corresponds to setting several transmitters of the same signal to the antenna ports p0 and p1 in the case of two transmitters, or p0 to p3 in the case of four transmitters to support the transmission diversity which facilitates the improvement of the quality of the received signal.

In the case of transmission using two antenna ports p0 and p1, the transmission diversity corresponds to the space-frequency block coding (SFBC). In the case of transmission using four antenna ports p0 to p3, the transmission diversity corresponds to the SFBC/FSTD (Frequency Shift Transmit Diversity) mechanism.

Transmission mode 3 (TM3) is specified for open-loop SU-MIMO. It corresponds to setting two transmitters of different signals and two receivers (SU-MIMO 2×2) using the antenna ports p0 and p1, or four transmitters and four receivers (SU-MIMO 4×4) using the antenna ports p0 to p3.

TM3 supports the spatial multiplexing function with an open-loop control which facilitates the improvement of the throughput of the cell.

TM3 uses a precoding matrix with cyclic delay diversity (CDD). The CDD method consists of applying a fixed precoding, the possible values of which are defined in a codebook.

Transmission mode 4 (TM4) is specified for closed-loop SU-MIMO. It corresponds to setting two transmitters of different signals and two receivers (SU-MIMO 2 × 2) using the antenna ports p0 and p1, or four transmitters and four receivers (SU-MIMO 4 × 4) using the antenna ports p0 to p3.

TM4 supports the spatial multiplexing function in a closed loop. The mobile transmits in the PMI the pre-encoding index selected in the codebook.

Transmission mode 5 (TM5) is specified for MU-MIMO. It supports the spatial multiplexing function with a closed-loop control, for two users (MU-MIMO 2 × 2) or four users (MU-MIMO 4 × 4).

Transmission mode 6 (TM6) corresponds to a simplified version of TM4, for which a single spatial layer is used.

Transmission mode 7 (TM7) supports the beamforming function. This mode uses the antenna port p5.

TM7 can also simultaneously support the MU-MIMO function, for providing spatial multiplexing of several users in an open loop, with each user granted one layer.

TM7 is suitable for the time-division duplex (TDD), for which the sharing between the transmission for the upstream and downstream directions takes place temporally.

Transmission mode 8 (TM8) is an extension of TM7. The spatial multiplexing allows the following configurations:

– two users with an allocation of two spatial layers per user;

– four users with an allocation of one spatial layer per user.

TM8 uses the antenna ports p7 and p8.

Transmission mode 9 (TM9) is configured either for SU-MIMO 8 × 8, for beamforming or for MU-MIMO. TM9 is associated with the antenna ports p7 to p14.

Transmission mode 10 (TM10) is similar to TM9. The main difference comes from CoMP (Coordinated Multi Point) transmission, for which the transmitting antennas can be physically located on different sites.

Table 2.5 summarizes the various modes of transmission, the evolved node base station (eNB) being able to switch between several transmission modes.

Mode	Transmission scheme
1	SISO, antenna port p0
2	Transmit diversity (MISO)
3	Transmit diversity (MISO)
	SU-MIMO, open loop
4	Transmit diversity (MISO)
	SU-MIMO, closed loop
5	Transmit diversity (MISO)
	MU-MIMO
6	Transmit diversity (MISO)
	SU-MIMO, closed loop one spatial layer
7	Transmit diversity (MISO) or SISO, antenna port p0
	Beamforming and MU-MIMO antenna port p5
8	Transmit diversity (MISO) or SISO, antenna port p0
	Beamforming and MU-MIMO antenna ports p7 and p8
9	Transmit diversity (MISO) or SISO, antenna port p0
	Beamforming and MU-MIMO antenna ports p7 to p14
10	Transmit diversity (MISO) or SISO, antenna port p0
	Beamforming and MU-MIMO antenna ports p7 to p14 CoMP

Table 2.5. *Downlink transmission modes*

The correspondence between the antenna configuration, described in section 2.3, and the transmission modes is given in Table 2.6.

Antenna configuration	Transmission modes
A	TM1
B	TM5, TM7 for TDD
C	TM5, TM7 to TM8 for TDD
D	TM2 to TM4, TM6
E	TM2 to TM6, TM7 to TM8 for TDD
F	TM2 to TM6
G	TM2 to TM6, TM7 to TM8 for TDD, TM9
H	TM2 to TM6
I	TM2 to TM4, TM6

Table 2.6. *Correspondence between the configuration of the antennas and modes of transmission*

2.4.2. *Uplink*

Since the mobile is equipped with two antennas, the transmission can be carried out on one of the two antennas; the selection of the antenna is performed either by the mobile or by the eNB entity. If the eNB entity is equipped with two receptors, it can implement the reception diversity.

Transmission mode 1 (TM1) is the SISO type. It corresponds to setting a transmitter to the antenna port p10 for the PUSCH or to the antenna port p100 for the PUCCH.

Transmission mode 2 (TM2) is the MIMO type for the PUSCH. It corresponds to setting two transmitters of different signals on the antenna ports p20 and p21 (MIMO 2×2) or four transmitters on the antenna ports p40 to p43 (MIMO 4×4) to support the spatial multiplexing in a closed loop.

TM2 uses transmit diversity for the PUCCH. It corresponds to setting two transmitters of the same signal on the antenna ports p200 and p201.

2.5. FD-MIMO mechanism

The elevation beamforming (EBF) allows a beam to be directed in a specific manner, for example a beam pointing either to the top or to the bottom. This technique contrasts with conventional antennal systems for which the tilt angle is fixed.

The FD-MIMO (Full-Dimension MIMO) mechanism is based on the elevation beamforming in the vertical plane and in the horizontal plane (Figure 2.5). Both directions can be combined, leading to two-dimensional beamforming.

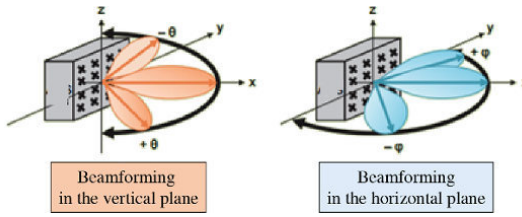

Figure 2.5. *Beamforming in different planes*
(source: NTT DOCOMO Technical Reports Journal, vol. 18 no. 2)

This new beamforming technique tends to increase the number of antennas since the signal has spatial access to more degrees of freedom. It is implemented by an active antenna system (AAS).

The AAS consists of a block of TXU transmitters and TRU receivers, a radio distribution network (RDN) and an antenna array (AA) (Figure 2.6).

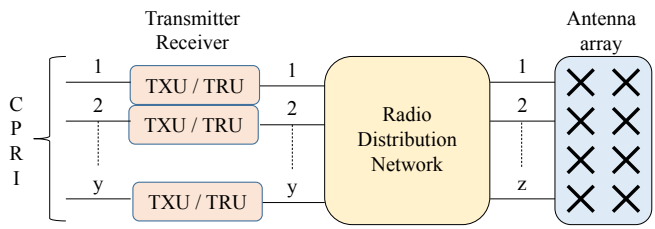

Figure 2.6. *AAS*

The transmitter block TXU takes the baseband signals delivered by the common public radio interface (CPRI) and outputs the radio frequency signals. Each baseband signal can be assigned to one or more TXU transmitters. The RF outputs are distributed to the antenna array via the radio distribution network (RDN). The receiver block TRU performs the reverse operation.

In order to provide an elevation of a zenith angle θ_{etilt}, the RDN weights the radio frequency signal supplied by the unit TXU by a coefficient w. The same operation is performed for the signal received from the antenna array.

The configuration of an antenna array is given by the parameters (M, N and P), where M is the number of antenna elements having the same polarization in each column (M = {1, 2, 4, 8}), N is the number of columns (N = {1, 2, 4, 8, 16}) and P is the number of polarizations (normally equal to 2).

M_{TXRU} is the number of TXU/TRU per column and polarization and N_{TXRU} is the number of TXU/TRU per row and polarization.

Two generic models of mapping between the antenna elements {M, N, P} and the TXU/TRU {M_{TXRU}, N_{TXRU}} have been defined: the sub-array partition model and the full-connection model.

For the sub-array partition model (Figure 2.7), the antenna elements are distributed among different groups and each TXU/TRU is connected to a group. The weighting value w_k of the radio signal is provided by the following formula:

$$w_k = \frac{1}{\sqrt{K}} \exp\left(-j \frac{2\pi}{\lambda} (k-1) d_v \cos\theta_{etilt} \right), \text{ for } k=1, 2, \ldots, K$$

where:

$$K = \frac{M}{M_{TXRU}};$$

λ is the wavelength;

d_v is the distance separating two antenna elements vertically;

θ_{etilt} is the zenith angle.

For the full-connection model (Figure 2.7), each TXU/TRU is connected to each antenna element. A combiner is used to couple the different TXU/TRU on each antenna element. The value of the weighting $w_{m,m'}$ of the radio signal is provided by the following formula:

$$w_{m,m'} = \frac{1}{\sqrt{M}} \exp\left(-j \frac{2\pi}{\lambda} (m-1) d_v \cos\theta_{etilt,m'} \right)$$

for $m=1, 2, \ldots, M$ and $m'=1, 2, \ldots, M_{TXRU}$

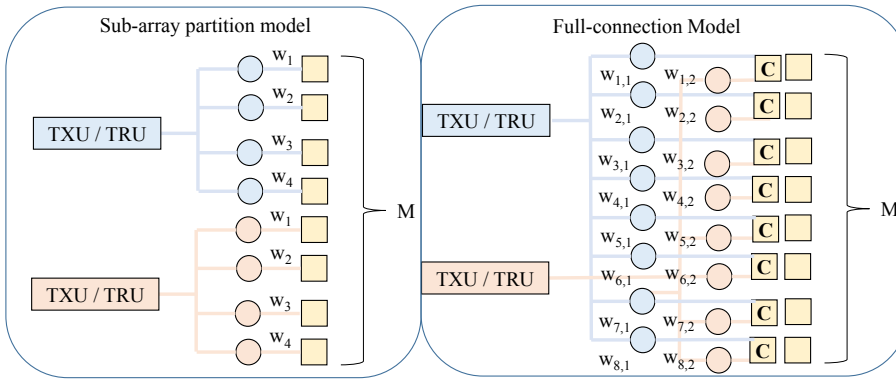

Figure 2.7. *Mapping between the TXU/TRU and the antenna elements*

The main changes in FD-MIMO compared to traditional MIMO are given in Table 2.7.

Mechanism	MIMO	FD-MIMO
Number of antenna ports CSI-RS	1, 2, 4, 8	1, 2, 4, 8, 12, 16
Beamforming	Horizontal plane	Horizontal and vertical planes
Number of radio signal SU-MIMO	8	8
Number of radio signal MU-MIMO	4 (note 1)	8 (note 2)

Note 1: the maximum number of mobiles spatially multiplexed is equal to 4. The number of radio signals per mobile is then equal to 2.

Note 2: the maximum number of mobiles spatially multiplexed is equal to 8. The number of radio signals per mobile is then equal to 2.

Table 2.7. *Comparison between MIMO and FD-MIMO*

The FD-MIMO mechanism introduces two methods for CSI feedback to the eNB entity: the Class A method and the Class B method.

The Class A method is applied to the sub-array partition model and consists of reassembling the CSI by antenna element and polarization of a group from the non-precoded CSI-RS.

The Class A method defines a number of non-precoded CSI-RS and a number of antenna ports that can vary from 1 to 16, which limits the configuration of the antenna, and adopts a codebook identical to the one defined for the transmission mode TM9, for each plane (horizontal or vertical).

The CSI-RS uses two resource elements for each antenna port. The use of the orthogonal covering code (OCC) makes it possible to consume only two resource elements for two antenna ports.

There are 40 resource elements reserved for mapping the CSI-RS:

– in the case of eight antenna ports, the CSI-RS consumes eight resource elements. There are therefore five different configurations;

– in the case of four antenna ports, the CSI-RS consumes four resource elements. There are therefore 10 different configurations.

Table 2.8 shows the constitution of the antenna ports to obtain the values equal to 12 and 16 from an aggregation of configurations.

Figure 2.8 shows a mapping of the CSI-RS on the resource elements, for 12 and 16 antenna ports.

Number of antenna ports	Number of antenna ports per configuration	Number of configurations
12	4	3
16	8	2

Table 2.8. *Constitution of the antenna ports: FD-MIMO*

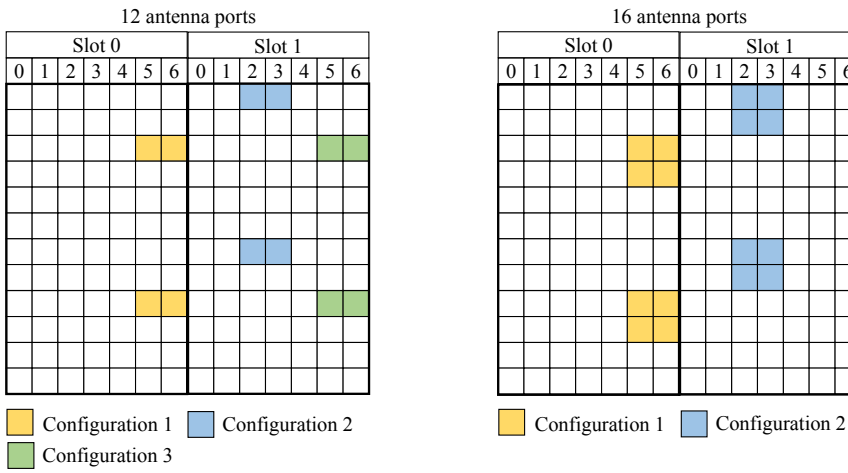

Figure 2.8. *CSI-RS mapping: FD-MIMO*

The Class B method is applied to the full-connection model and consists of reporting the CSI for each beam formed from the CSI-RS.

The Class B method limits the number of CSI-RS and the number of antenna ports to 8. This number is independent of the number of antenna elements used by the radio signal.

The reported CSI relates to the best received CSI-RS and contains a CSI resource index (CRI) corresponding to this CSI-RS.

2.6. eFD-MIMO mechanism

The eFD-MIMO (enhanced FD-MIMO) mechanism provides the following enhancements to the CSI-RS:

– increasing the number {20, 24, 28, 32} of reference signals;

– reducing the overhead introduced by the reference signals.

Table 2.9 shows the constitution of the antenna ports to obtain the values between 20 and 32 from an aggregation of configurations.

Number of antenna ports	Number of antenna ports per configuration	Number of configuration
20	4	5
24	8	3
28	4	7
32	8	4

Table 2.9. *Constitution of the antenna ports: eFD-MIMO*

Figure 2.9 shows a mapping of the CSI-RS on the resource elements, for 20 and 32 antenna ports. The overhead is equal to 11.9% (respectively 19%) for a number of CSI-RS equal to 20 (respectively 32).

Reducing the overhead consists of configuring the frequency density of the CSI-RS with a normal density of value 1 or with a reduced density of value {1/2, 1/3}.

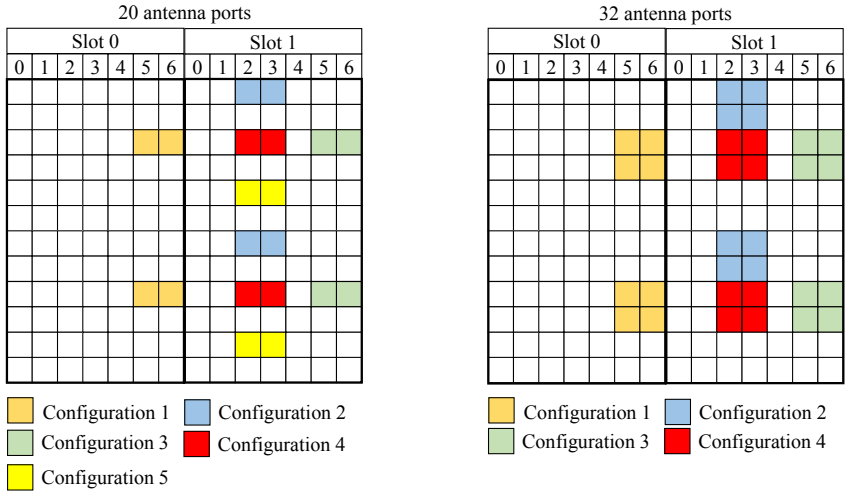

Figure 2.9. *CSI-RS reference signal mapping: eFD-MIMO*

The reduction of the overhead is achieved by transmitting the CSI-RS in one pair of resource blocks in two (density 1/2) or in three (density 1/3).

For the Class B method, the following mechanisms have been introduced to allow more efficient use of CSI-RS resources formed by a mobile-specific beam, for example, to enable more mobile to share a CSI-RS resource pool:

– aperiodic CSI-RS, wherein a mobile is configured to measure the CSI-RS in a given sub-frame;

– multi-shot CSI-RS, wherein a mobile is configured to measure the periodic CSI-RS for a determined period of time.

Two-step resource configurations, combining the use of RRC messages and MAC (Medium Access Control) elements, are introduced to allow flexible selection of resources while maintaining control over CSI reporting overhead.

The improvements also include the optimization of CSI reports obtained from CSI-RS measurements.

The first mechanism aims to improve the quality of CSI feedback by adopting a two-step CSI report. In the first step, CSI reporting is obtained from a non-precoded physical signal measurement (Class A method). In the second step, CSI reporting is obtained from a measurement of the CSI-RS formed by a beam (Class B method).

The second mechanism aims to provide greater flexibility in the use of CSI-RS resources with a limited number of CSI processes. CSI reporting is realized with one CSI process (Class B method) with K>1 CSI-RS resources for the first step and with K=1 CSI-RS resources for the second step.

3

MBB Service – Carrier Aggregation

3.1. Functional architecture

The aggregation of the carriers results in sharing of the IP (Internet Protocol) packets between the different accesses. For the downstream direction (respectively the upstream direction), the sharing is performed by the evolved node base station (eNB) (respectively the mobile) and the reassembly is provided by the mobile (respectively the entity eNB). This operation is performed exclusively in the evolved universal terrestrial radio access network (E-UTRAN).

LTE (Long-Term Evolution) aggregation operates in licensed frequency bands (Figure 3.1).

LAA (Licensed Assisted Access) aggregation is an extension of LTE aggregation. The LTE transmission, defined by the data link layer and the physical layer, takes place on LTE and Wi-Fi (Wireless Fidelity) frequency bands, between the mobile and the eNB entity, without an intermediate access point, in accordance with the 3GPP standards (Figure 3.1).

The LTE Advanced and LTE Advanced Pro evolutions respectively defined an aggregation of five channels in a licensed band and extend up to 32 channels in a non-licensed band (Figure 3.1).

LWA (LTE–Wi-Fi Aggregation) and LWIP (LTE/WLAN radio level integration with IPsec tunnel) aggregations use both LTE and Wi-Fi technologies in their respective bands. The transmission on the Wi-Fi radio channel occurs between the mobile and the access point (AP) in accordance with 802.11 standard (Figure 3.1).

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

LTE and Wi-Fi carrier aggregation can be implemented with collocated or remote eNB and AP entities. In the non-collocated case, the Xw interface is the point of reference between the eNB and AP entities (Figure 3.1).

The eNB entity is the anchor point for the data exchanged with the mobile, belonging to the user plane (the IP packets) and the control plane, and connects to the evolved packet core (EPC):

– at the level of the mobility management entity (MME), via the S1-MME interface, for the S1-AP signaling;

– at the level of the serving gateway (SGW), via the S1-U interface, for the S1 bearer.

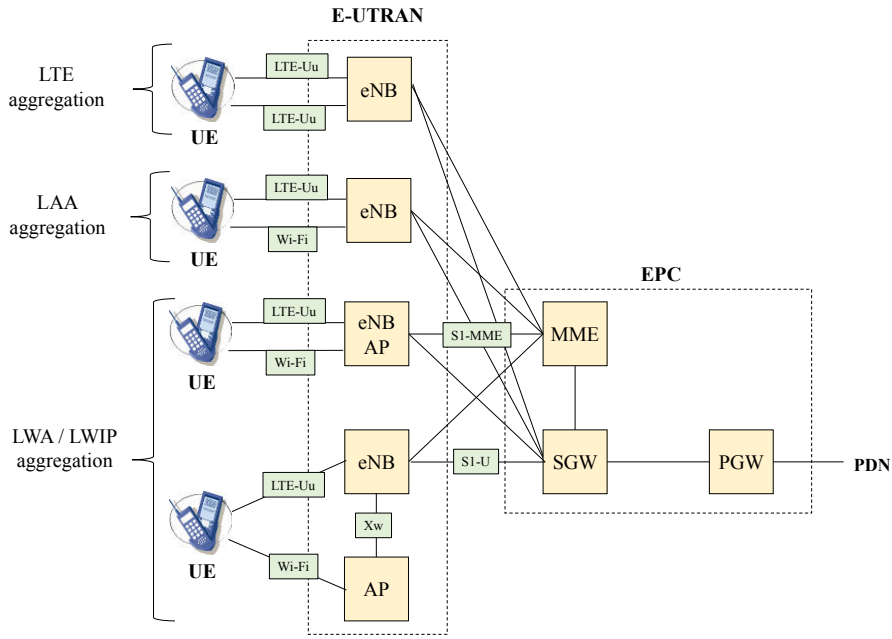

Figure 3.1. *Functional architecture for LTE and Wi-Fi carrier aggregation*

3.2. LTE aggregation

3.2.1. *Radio channels*

Carrier aggregation (CA) combines multiple component carriers (CC) and allows wider radio channel bandwidth in order to increase the throughput of the cell.

The bandwidth of the radio channel is limited to 20 MHz in the LTE release. Aggregation can be performed over five radio channels for LTE Advanced and up to 32 radio channels for LTE Advanced Pro, bringing the maximum bandwidth value to 100 MHz or 640 MHz, respectively.

The radio channels can be aggregated according to several patterns (Figure 3.2):

– the radio channels can be adjacent in the same frequency bands;

– the radio channels can be spaced out in the same frequency bands;

– the radio channels can be localized in different frequency bands.

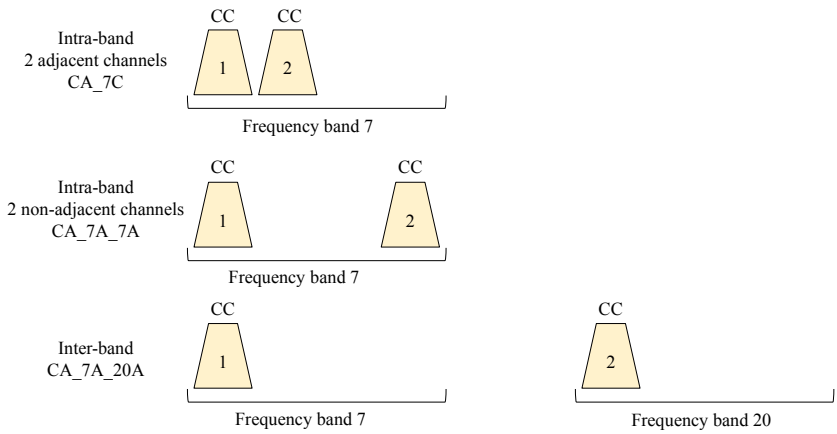

Figure 3.2. *Radio channel aggregation*

The notation relating to the radio channel aggregation determines the frequency band and the class of the bandwidth of the radio channel.

Class A corresponds to a bandwidth of the radio channel less than or equal to 20 MHz.

Class B corresponds to a bandwidth less than or equal to 20 MHz, obtained from the aggregation of two contiguous radio channels in the same frequency band.

Class C corresponds to a bandwidth less than or equal to 40 MHz, obtained from the aggregation of two contiguous radio channels in the same frequency band.

Class D corresponds to a bandwidth less than or equal to 60 MHz, obtained from the aggregation of three contiguous radio channels in the same frequency band.

Class E corresponds to a bandwidth less than or equal to 80 MHz, the number of concatenated radio channels in the same frequency band not being specified.

Class F corresponds to a bandwidth less than or equal to 100 MHz, the number of radio channels concatenated in the same frequency band not being specified.

One of the radio channels is the primary cell (PCell), and it has the following characteristics:

– the mechanisms for random access and RRC (Radio Resource Control) connection, which only occur on the primary cell;

– the NAS (Non-Access Stratum) messages related to the mobility and the session management, which are only transmitted in the primary cell;

– the IP packet from the user plane.

The other radio channels are the secondary cells (SCell) which only transmit IP packets from the traffic plane.

The bearer for both directions of transmission uses two paired bandwidths in the FDD (Frequency-Division Duplex) mode or a single bandwidth in the TDD (Time-Division Duplex) mode.

For the FDD mode, each direction of transmission operates simultaneously in the assigned radio channel in the frequency band.

For the TDD mode, the two directions of transmission operate in the same radio channel, each direction being assigned during a portion of the time.

The carrier aggregation can associate radio channels operating in the FDD and TDD modes.

3.2.2. *PDCCH physical channel*

The physical downlink control channel (PDCCH) carries the downlink control information (DCI) for one or more user equipment (UE):

– resource allocation, modulation and coding schemes of the data transmitted in the physical downlink shared channel (PDSCH) and in the physical uplink shared channel (PUSCH);

– transmit power control of the physical uplink control channel (PUCCH) and the PUSCH.

For each sub-frame, the PDCCH is mapped on the first, the first two or the first three OFDM (Orthogonal Frequency-Division Multiplexing) symbols.

The number of OFDM symbols allocated to the PDCCH is indicated in the physical control format indicator channel (PCFICH).

As part of the carrier aggregation, the PDCCH can either carry the scheduling information for the radio channel where it is transmitted or allocate resources for other radio channels in the case of inter-carrier scheduling.

The inter-carrier scheduling makes it possible to avoid inter-cell interference over the PDCCH by allocating resources to the adjacent cells over different radio channels.

The inter-carrier scheduling can only be applied to the secondary channels (SCell), since the primary channel (PCell) systematically has one PDCCH allocated.

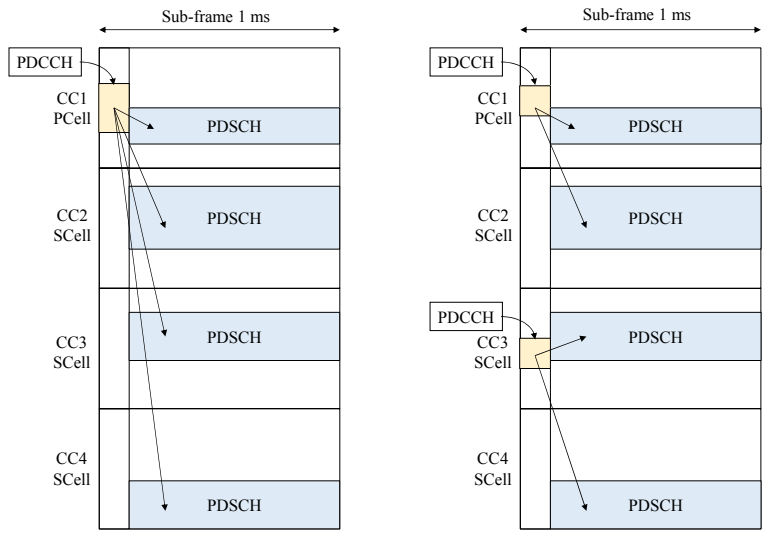

Figure 3.3. *Inter-carrier scheduling*

The inter-carrier scheduling can be established in accordance with two scenarios (Figure 3.3):

– the PDCCH is only carried by the primary radio channel (PCell);

– the PDCCH is carried by the primary radio channel (PCell) and the secondary radio channel (SCell).

3.2.3. *MAC layer*

3.2.3.1. *HARQ mechanism*

The medium access control (MAC) provides the management of retransmission in the case of error via the HARQ (Hybrid Automatic Repeat reQuest) mechanism, established at the level of the physical layer.

The radio channel aggregation impacts the MAC layer which must handle a HARQ mechanism for each radio channel.

3.2.3.2. *Control elements*

The PHR (Power HeadRoom) is a MAC control element which contains the indication of the mobile power reserve, the difference between maximum power and power used for the PUSCH.

The PHR control element is periodically transmitted by the mobile, and the periodicity is indicated in the RRC *ConnectionSetup* or *ConnectionReconfiguration* message transmitted by the eNB entity.

The PHR control element is also transmitted when the variation of the attenuation due to propagation is greater than a threshold indicated in the same RRC messages.

The radio channel aggregation has introduced a new PHR control element to indicate the power reserve for each radio channel of the aggregation.

The radio channel aggregation has also introduced the ADM (Activation/Deactivation MAC) control element which concerns activation and deactivation of the SCell secondary radio channels.

The ADM control element is used when radio channels have been previously established by an RRC *ConnectionSetup* or *ConnectionReconfiguration* message.

The ADM control element makes it possible to save mobile consumption, and rapid deactivation of a secondary channel (SCell) allows the mobile to avoid processing relating to the bearer built on that channel.

3.2.4. *Mobile categories*

The mobile categories determine the maximum data rate on the LTE-Uu radio interface, for the downlink and the uplink.

The maximum rate depends on the optimal characteristics of the radio interface (modulation, radio channel bandwidth, MIMO mechanism) and the mobile's ability to handle the bit rate allowed by the radio conditions.

Mobile categories 1 to 5 are LTE mobiles defined in release 8 (Table 3.1).

Categories	1	2	3	4	5
DL rate (Mbps)	10	50	100	150	300
UL rate (Mbps)	5	25	50	50	75
Bandwidth (MHz)	20	20	20	20	20
Modulation DL	64-QAM	64-QAM	64-QAM	64-QAM	64-QAM
Modulation UL	16-QAM	16-QAM	16-QAM	16-QAM	64-QAM
MIMO DL	n.a.	2 × 2	2 × 2	2 × 2	4 × 4
MIMO UL	n.a.	n.a.	n.a.	n.a.	n.a.

DL: downlink; UL: uplink.

Table 3.1. *LTE mobile categories from release 8*

Mobile categories 6 to 12 are LTE Advanced mobiles defined in release 11 (Table 3.2).

Given the difficulty of processing the MIMO 4 × 4 for the mobile category 5, the mobile categories 6 and 7 were introduced to reach the bit rate of 300 Mbps for the downlink. Such performance is obtained by maintaining the MIMO 2 × 2 and doubling the bandwidth of the radio channel.

The mobile categories 9 and 10 (respectively 11 and 12) have a maximum bit rate of 450 Mbps (respectively 600 Mbps), obtained by the aggregation of three radio channels (respectively four radio channels), while retaining the MIMO 2 × 2.

The mobile categories 7, 10 and 12 can exceed the bit rate of 75 Mbps of the mobile category 5 for the uplink by doubling the bandwidth of the radio channel and avoiding the use of 64-QAM (Quadrature Amplitude Modulation).

Categories	6	7	8	9	10	11	12
DL rate (Mbps)	300	300	3000	450	450	600	600
UL rate (Mbps)	50	100	1500	50	100	50	100
Bandwidth (MHz)	2 × 20 DL	2 × 20 DL UL	5 × 20 DL UL	3 × 20 DL	3 × 20 DL 2 × 20 UL	4 × 20 DL	4 × 20 DL 2 × 20 UL
Modulation DL	64-QAM	64-QAM	64-QAM	64-QAM	64-QAM	64-QAM	64-QAM
Modulation UL	16-QAM	16-QAM	64-QAM	16-QAM	16-QAM	16-QAM	16-QAM
MIMO DL	2 × 2	2 × 2	8 × 8	2 × 2	2 × 2	2 × 2	2 × 2
MIMO UL	n.a.	n.a.	4 × 4	n.a.	n.a.	n.a.	n.a.

Table 3.2. *LTE Advanced mobile categories*

Release 12 introduced a separation of categories for downlink and uplink. The mobile is characterized by a combination of two categories.

Table 3.3 describes the mobile characteristics for the downlink, for 256-QAM and for the maximum bandwidth. The same bit rate can be achieved by decreasing the bandwidth and increasing the number of MIMO layers.

The mobile category 13 has the same characteristics in terms of bandwidth and MIMO as the mobile categories 5, 6 and 7, the increase in the bit rate being explained by the gain of the modulation.

The mobile category 14 has the same characteristics in terms of bandwidth and MIMO as the mobile category 8, the increase in the bit rate being explained by the gain of the modulation.

The mobile category 15 has the same characteristics in terms of bandwidth and MIMO as the mobile categories 11 and 12, the increase in the bit rate being explained by the gain of the modulation.

Categories	13	14	15	16	17	18	19	20
Rate (Mbps)	400	4000	800	1000	25000	1200	1600	2000
Bandwidth (MHz)	20 or 2 × 20	5 × 20	4 × 20	5 × 20	32 × 20	6 × 20	8 × 20	8 × 20
Modulation	256-QAM	256-QAM	256-QAM	256-QAM	256-QAM	256-QAM	256-QAM	256-QAM
MIMO	4 × 4 or 2 × 2	4 × 4	2 × 2	2 × 2	8 × 8	2 × 2	2 × 2	Note

Note: the 2-Gbps rate is achieved by 2 × 2 MIMO for six radio channels and 4 × 4 MIMO for the remaining two radio channels.

Table 3.3. *Mobile categories for the downlink from release 12*

Table 3.4 describes the characteristics of mobiles for the uplink.

Categories	13	14	15	16	17	18	19	20	21
Rate (Mbit/s)	150	9600	225	100	2100	200	13500	300	300
Bandwidth (MHz)	2 × 20	32 × 20	3 × 20	20	5 × 20	2 × 20	32 × 20	3 × 20	4 × 20
Modulation	64-QAM	64-QAM	64-QAM	256-QAM	256-QAM	256-QAM	256-QAM	256-QAM	64-QAM
MIMO	n.a.	4 × 4	n.a.	n.a.	4 × 4	n.a.	4 × 4	n.a.	n.a.

Table 3.4. *Mobile categories for the uplink from release 12*

3.3. LAA aggregation

The LAA mechanism exploits the U-NII (Unlicensed National Information Infrastructure) band at 5 GHz to transmit an LTE signal that is compliant with 3GPP specifications.

The radio channel operating in the licensed frequency band, used as the primary channel (PCell), supports the data of the control plane and the user plane.

The radio channel operating in the U-NII band, used as the secondary channel (SCell), only supports the data of the user plane.

3.3.1. *Frame structure*

The type-1 frame structure defined for the FDD mode lasts 10 ms and contains 10 sub-frames. Each sub-frame is made up of two time slots (Figure 3.4).

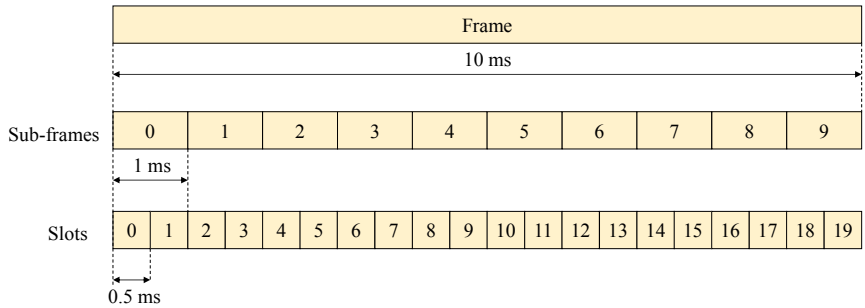

Figure 3.4. *Structure of type-1 frame*

The type-2 frame structure defined for the TDD mode also lasts 10 ms and contains two semi-frames of 5 ms each (Figure 3.5).

Each half-frame consists of five sub-frames and the second can correspond to a special sub-frame containing three particular fields:

– a field for the downlink pilot time slot (DwPTS) in the downlink. This field can contain data;

– a field for the uplink pilot time slot (UpPTS) in the uplink. This field can contain data or a preamble for the random access;

– a time of gap period (GP) between the two preceding fields. This interval time facilitates the compensation of a time difference between different mobiles and avoids an overlap between the two transmission directions.

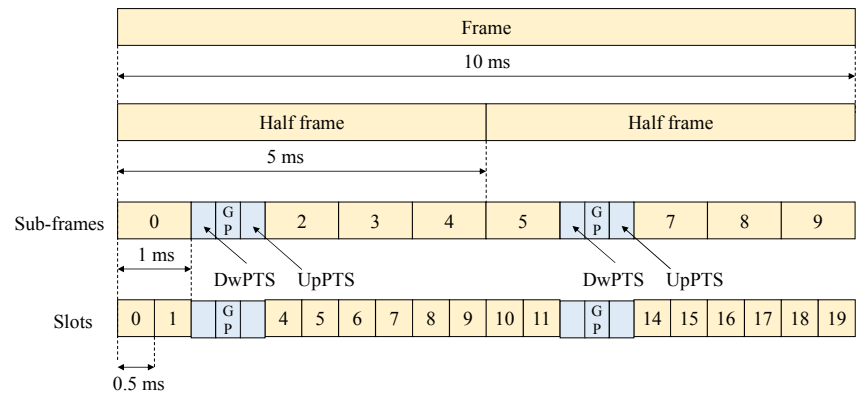

Figure 3.5. *Structure of type-2 frame*

The sub-frames are attributed to the data for the uplink and downlink according to diverse configurations (Table 3.5):

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) sub-frame attributed to the downlink;
U (uplink) sub-frame attributed to the uplink;
S (special) sub-frame containing the three particular fields.

Table 3.5. *Type-2 frame configuration*

– sub-frames 0 and 5 are always allocated to traffic in the downlink;

– sub-frame 1 is always allocated to the special sub-frame containing the three particular fields;

– sub-frame 2 is always allocated to traffic in the uplink;

– sub-frame 6 can be allocated to the special sub-frame containing three particular fields for a periodicity of 5 ms;

– sub-frames 3, 4, 7, 8 and 9 are allocated to the downlink or uplink traffic according to the selected configuration.

The type-3 frame is applicable for LAA aggregation. It also has a duration of 10 ms. The 10 sub-frames constituting the frame are available for transmission on the downlink.

The transmission may occupy one or more consecutive sub-frames, starting anywhere in a frame and ending with the last sub-frame containing either traffic or the downstream pilot DwPTS.

The eLAA (enhanced LAA) aggregation allows the mobile to use Wi-Fi access in both directions of transmission.

3.3.2. *Access to the radio channel*

The mechanism to access the radio channel is different for the LTE and Wi-Fi interfaces. For the LTE radio interface, access to the radio channel is controlled by the eNB entity. For the Wi-Fi radio interface, access to the radio channel uses the CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) mechanism.

To avoid interference with other Wi-Fi interfaces, the eNB entity or the mobile applies the LBT (Listen Before Talk) mechanism before transmitting in the U-NII radio channel. The equipment uses energy sensing to determine the presence or absence of other signals on the radio channel during the CCA (Clear Channel Assessment) observation time.

The LBT mechanism has two options: frame-based equipment (FBE) and load-based equipment (LBE).

For the FBE option, the equipment operates on the basis of a synchronization with a fixed frame period. At the end of the frame period, the equipment performs a CCA check on the radio channel. If the channel is free, then the data is transmitted immediately to the beginning of the next frame. If the channel is busy, then another CCA check is performed at the next frame period (Figure 3.6).

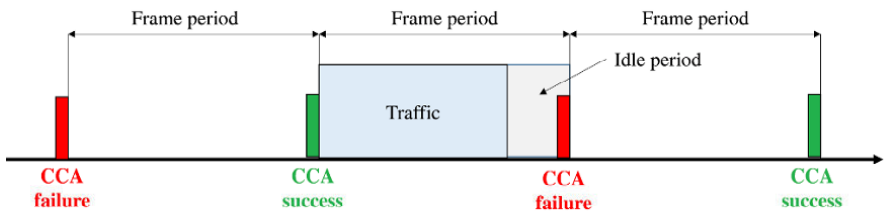

Figure 3.6. *LBT mechanism: FBE option*

For the LBE option, the device performs CCA control whenever there is data to transmit. If the channel is free, then the data is transmitted immediately. If the channel is busy, then the device must wait until the timer for the backoff mechanism expires (Figure 3.7). This timer is decremented when the radio channel is free.

The LBE option is relatively similar to the backoff mechanism of Wi-Fi access. Unlike Wi-Fi access, which adopts an exponential backoff mechanism, the LBE option opts for a backoff mechanism with a fixed window.

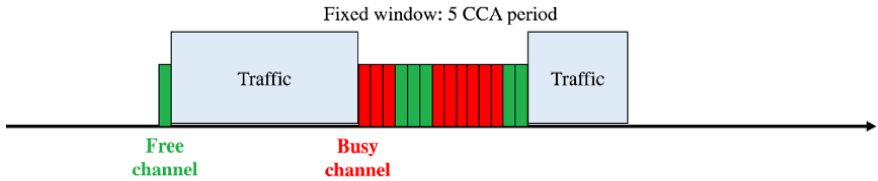

Figure 3.7. *LBT mechanism: LBE option*

3.3.3. *Discovery reference signal (DRS)*

The small cell usually deployed as a secondary cell (SCell) does not need to be permanently activated. In this case, a mobile cannot perform quality measurements on this cell.

The discovery reference signal (DRS) has therefore been introduced and includes the following signals:

– the primary synchronization signal (PSS) ensuring the frequency synchronization and some of the time synchronization;

– the secondary synchronization signal (SSS) completing the time synchronization. The two physical signals PSS and SSS make it possible to determine the physical-layer cell identity (PCI);

– the cell-specific reference signal (CRS) used to calculate the transfer function of the radio channel and to make the coherent demodulation of the received signal. The CRS also makes it possible to measure the reference signal received power (RSRP) and the reference signal received quality (RSRQ).

The reference signal is transmitted with a period of 40, 80 or 160 ms. Only one sub-frame and only the first 12 OFDM symbols of this sub-frame are used to transmit the DRS.

The reference signal can be transmitted in any sub-frame during the discovery measurement timing configuration (DMTC) which lasts 6 ms. The DMTC is shifted by a dmtcOffset value relative to the start of the frame.

The reference signal can be incorporated in the PDSCH when there is data to be transmitted.

3.4. LWA aggregation

3.4.1. *Protocol architecture*

LWA aggregation occurs at the PDCP layer. The eNB entity carries out a switching of the bearers between, on the one hand, the S1 bearers and, on the other hand (Figures 3.8 and 3.9):

– the LTE bearer, for which the data only transits on the LTE access;

– the shared LWA bearer, for which the data can pass on both LTE and Wi-Fi accesses;

– the switched LWA bearer, for which the data only passes over the Wi-Fi access.

The LWA bearer is controlled by the eNB entity from measurement reports transmitted by the mobile.

The PDCP frames transmitted over the Wi-Fi access are encapsulated by an LWAAP (LWA Adaptation Protocol) header containing the logical channel identifier (LCID) of the radio bearer.

On LTE access, the LCID is carried by the MAC layer. The recipient uses the LCID to reassemble the PDCP frames of the same bearer.

The re-sequencing of the PDCP frames received by the LTE and Wi-Fi accesses is performed by the PDCP.

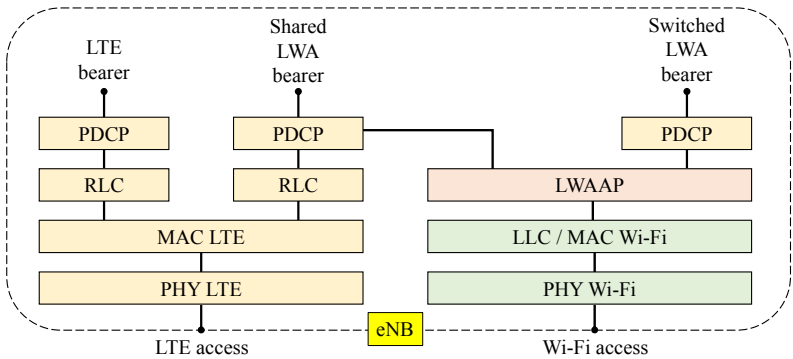

Figure 3.8. *Protocol architecture for LWA: collocated eNB and AP entities*

Frames transported on an LWA bearer are only these acknowledged, these frames corresponding to RLC frames using the acknowledged mode (AM) on the LTE interface.

The type field of the LLC header for Wi-Fi access is set to hexadecimal 9E65. The mobile uses this value to determine that the frame comes from an LWA bearer.

When the eNB and AP entities are distant, the eNB entity can be connected to multiple AP entities via the Xw interface that supports the traffic and control data (Figure 3.9).

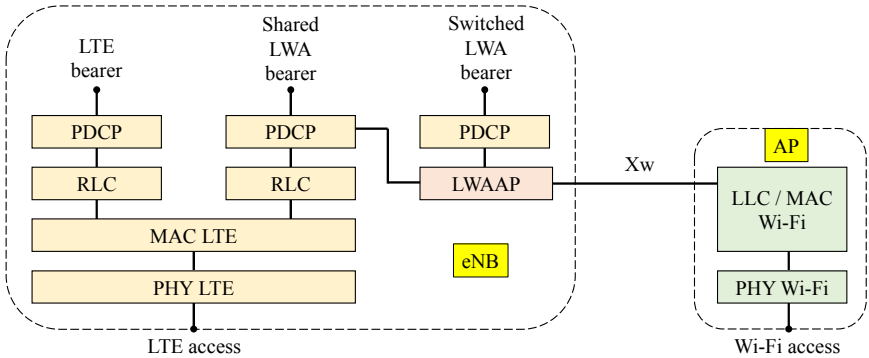

Figure 3.9. *Protocol architecture for LWA: distant eNB and AP entities*

The NAS signaling data is carried on the S1-MME interface, between the MME and eNB entities, and then on the Xw-C (Control) interface, between the eNB and AP entities.

Traffic data, corresponding to the IP stream, is transported in a GTP-U (GPRS Tunneling Protocol User) tunnel:

– on the S1-U interface, between the SGW and eNB entities;

– on the Xw-U (User) interface, between the eNB and AP entities.

3.4.2. *Procedures*

3.4.2.1. *WT Addition procedure*

The WT Addition procedure is initialized by the eNB entity and is used to establish the mobile context at the access point (AP) to provide mobile resources over the Wi-Fi interface (Figure 3.10).

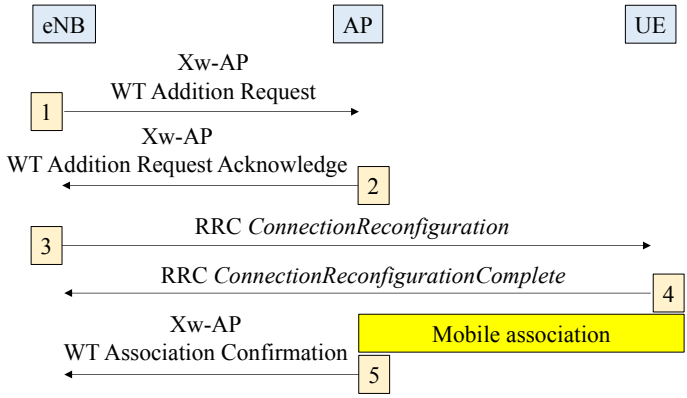

Figure 3.10. *WT Addition procedure*

1) The eNB entity transmits to the access point (AP) the message Xw-AP WT Addition Request in order to allocate resources to the mobile, indicating the characteristics of the LWA bearer.

2) If the access point can accept the resource request, it responds with the message Xw-AP WT Addition Request Acknowledge.

3) The eNB entity sends the message RRC *ConnectionReconfiguration* to the mobile, indicating the configuration of the radio resource.

4) The mobile applies the new configuration and responds to the eNB entity with the message RRC *ConnectionReconfigurationComplete*.

5) The mobile associates with the access point which then transmits the message Xw-AP WT Association Confirmation to the eNB entity.

3.4.2.2. *WT Modification procedure*

The WT Modification procedure can be initialized either by the eNB entity or by the access point and can be used to modify, set or release bearer contexts or to modify other properties of the mobile context.

The WT Modification procedure initiated by the eNB entity is described in Figure 3.11.

1) The eNB entity sends the message Xw-AP WT Modification Request to request the access point to modify the specific bearer resources.

2) If the access point accepts the request, it applies the configuration modification to the resource and responds with the message Xw-AP WT Modification Request Acknowledge.

3) If the modification requires a new configuration for the mobile, the eNB entity sends the RRC *ConnectionReconfiguration* message, including the new configuration of the Wi-Fi radio resource.

4) The mobile applies the new configuration and responds with the message RRC *ConnectionReconfigurationComplete*.

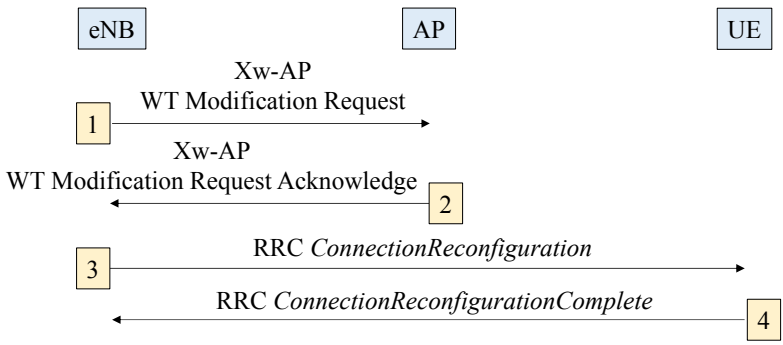

Figure 3.11. *WT Modification procedure initiated by the eNB entity*

The WT Modification procedure initiated by the access point is described in Figure 3.12.

1) The access point sends the message Xw-AP WT Modification Required to the eNB entity to modify the radio resources of the Wi-Fi access.

2) The eNB responds with the message Xw-AP WT Change Confirm.

3) If the modification requires a new configuration for the mobile, the eNB entity sends the message RRC *ConnectionReconfiguration*, including the new configuration of the Wi-Fi radio resource.

4) The mobile applies the new configuration and responds with the message RRC *ConnectionReconfigurationComplete*.

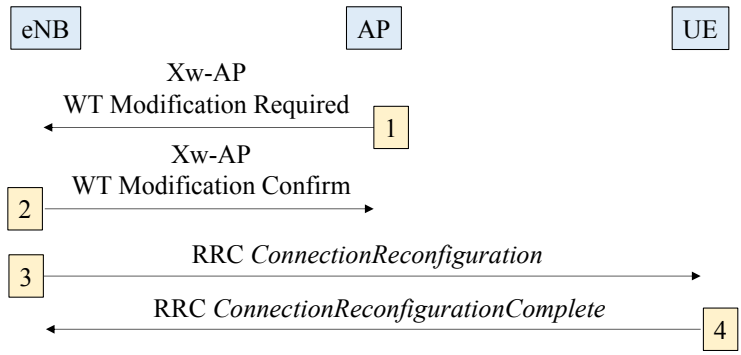

Figure 3.12. *WT Modification procedure initiated by the access point*

3.4.2.3. *WT Release procedure*

The WT Release procedure can be initialized either by the eNB entity or by the access point and is used to initiate the release of the mobile context at the access point. The recipient cannot reject the request.

The WT Release procedure initiated by the eNB entity is described in Figure 3.13.

1) The eNB entity sends the message Xw-AP WT Release Request to request the Wi-Fi access point to release the allocated radio resources over the Wi-Fi access.

2) If necessary, the eNB entity sends the message RRC *ConnectionReconfiguration* to the mobile, indicating the release of the radio resources.

3) The mobile responds with the message RRC *ConnectionReconfigurationComplete*.

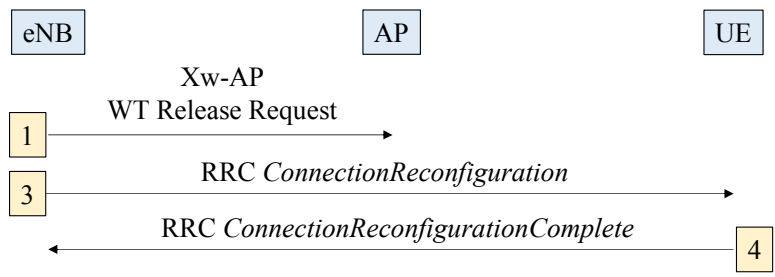

Figure 3.13. *WT Release procedure initiated by the eNB entity*

The WT Release procedure initiated by the access point is described in Figure 3.14.

1) The access point sends the message Xw-AP WT Release Required to the eNB entity to request the release of radio resources from the Wi-Fi access.

2) The eNB entity responds with the message Xw-AP WT Release Confirm.

3) If necessary, the eNB entity sends the message RRC *ConnectionReconfiguration* to the mobile, indicating the release of the radio resources.

4) The mobile responds with the message RRC *ConnectionReconfigurationComplete*.

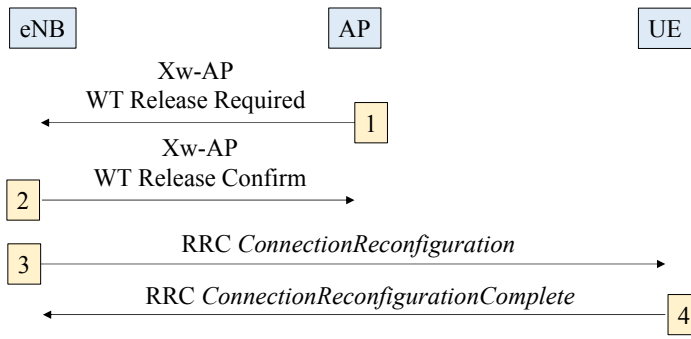

Figure 3.14. *WT Release procedure initiated by the access point*

The procedure for changing the access point is initiated by the eNB entity and used to transfer the mobile context from a source AP to a target AP. This procedure is performed using the WT Release and WT Addition procedures.

3.5. LWIP aggregation

3.5.1. *Protocol architecture*

The LWIP aggregation only applies to the IP packets of the S1 bearer. The RRC (Radio Resource Control) and signaling messages, which are exchanged between the mobile and the eNB entity, are carried on the LTE interface (Figure 3.15).

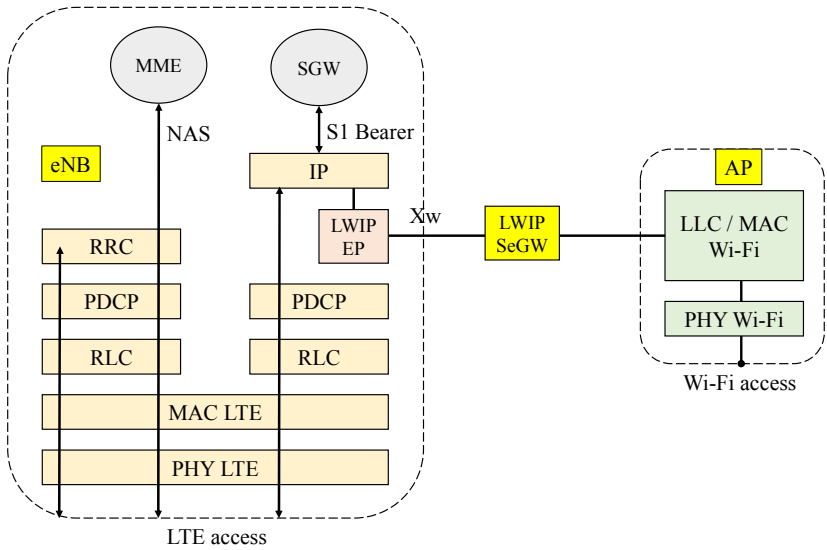

Figure 3.15. *Protocol architecture for the LWIP aggregation*

IP packets are transported between the eNB entity and the mobile in the LWIP tunnel. The LWIPEP (LWIP Encapsulation Protocol) header contains the LCID of the radio bearer.

The LWIP tunnel is protected between the mobile and the security gateway (SeGW) through an IP Security (IPSec) mechanism. Only one IPSec mechanism is mounted for all LWIP tunnels.

The LWIP tunnel is transmitted in a GTP-U tunnel on the Xw interface, between the eNB and the SeGW entities.

The IKE procedure for the IPSec mechanism is initialized after the association of the mobile with the Wi-Fi access point and authentication based on the EAP-AKA (Extensible Authentication Protocol–Authentication and Key Agreement) method.

Each bearer is configured so that the downstream direction, the upstream direction or both directions of transmission pass through the tunnel protected by the IPSec mechanism.

For the downstream, IP packets are transmitted either on the LTE interface only or on the Wi-Fi interface only, or simultaneously on both LTE and Wi-Fi interfaces. In the latter case, the mobile can receive IP packets out of sequence.

For the upstream, IP packets are transmitted either on the LTE interface only or on the Wi-Fi interface only.

3.5.2. *Tunnel establishment*

The procedure for establishing the LWIP and IPSec tunnels is described in Figure 3.16.

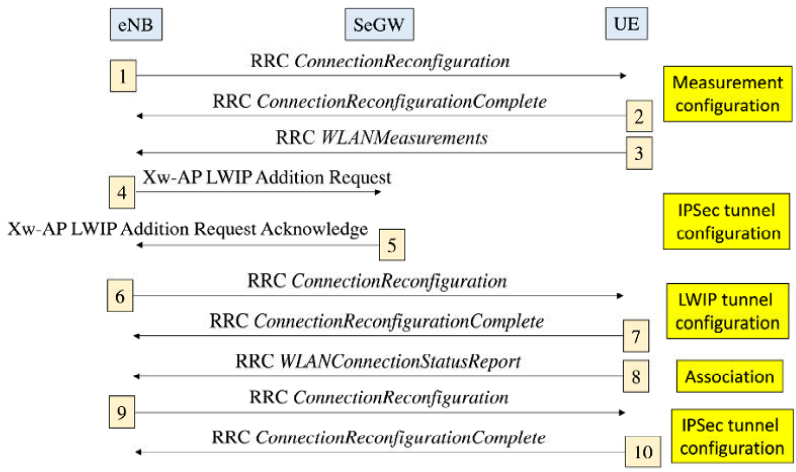

Figure 3.16. *LWIP and IPSec tunnel establishment*

1) The eNB entity configures the mobile with the message RRC *ConnectionReconfiguration* to perform measurements on Wi-Fi access in order to start the LWIP and IPSec tunnel establishment.

2) The mobile applies the new configuration and responds with the message RRC *ConnectionReconfigurationComplete*.

3) The mobile sends to the eNB entity the message RRC *WLANMeasurements* containing the measurements performed on the Wi-Fi access.

4) The eNB entity sends the message Xw-AP LWIP Addition Request to request the security gateway (SeGW) to allocate resources for IPSec tunnel establishment.

5) If the security gateway accepts the request, it responds with the message Xw-AP LWIP Addition Request Acknowledge.

6) The eNB entity sends the message RRC *ConnectionReconfiguration* to the mobile to establish the LWIP tunnel.

7) The mobile applies the new configuration and responds with the message RRC *ConnectionReconfigurationComplete*.

8) The mobile sends the confirmation of the association with the Wi-Fi access point to the eNB entity in the message RRC *WLANConnectionStatusReport*.

9) The eNB entity sends the message RRC *ConnectionReconfiguration* to the mobile to establish the IPSec tunnel and can configure the bearers that will use the IPSec tunnel.

10) The mobile applies the new configuration and responds with the message RRC *ConnectionReconfigurationComplete*.

4

Wi-Fi Integration – Network Architecture

4.1. Functional architecture

EPS (Evolved Packet System) is the name of the 4G mobile network. It consists of an evolved packet core (EPC) and an evolved universal terrestrial radio access network (E-UTRAN).

The E-UTRAN presents the LTE (Long-Term Evolution) radio interface to the mobile.

Wi-Fi (Wireless Fidelity) interface is subsequently integrated into the EPS network and it is a component of a set of technologies grouped under the term Non-3GPP Access.

Its introduction has an impact on the core network (EPC) architecture, which has several variants depending on the following characteristics:

– Wi-Fi access is trusted or untrusted by the operator;

– mobility is managed by the network or the mobile.

4.1.1. *Architecture based on the S2a interface*

The functional architecture based on the S2a interface corresponds to trusted Wi-Fi access and network-based mobility (Figure 4.1).

The mobile data stream travels through the Wi-Fi radio interface and the S2a tunnel to access the packet data network (PDN). The PGW (PDN Gateway) entity is an IP (Internet Protocol) router that acts as a gateway for the mobile data stream.

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

The home subscriber server (HSS) and the AAA (Authentication, Authorization and Accounting) server provide the following functions:

– mutual authentication of the mobile and the AAA server via the SWx and STa interfaces. This authentication has the effect of opening Wi-Fi access to the mobile;

– transfer of the mobile profile to the PGW entity via the S6b interface and to the trusted Wi-Fi access via the STa interface. The mobile profile contains a list of access point names (APN) and the quality of service (QoS) level of the S2a tunnel and Wi-Fi interface.

The policy and charging rules function (PCRF) also provides the traffic profile, including the QoS level of the S2a tunnel, to the PGW entity via the Gx interface and to the trusted Wi-Fi access via the Gxa interface.

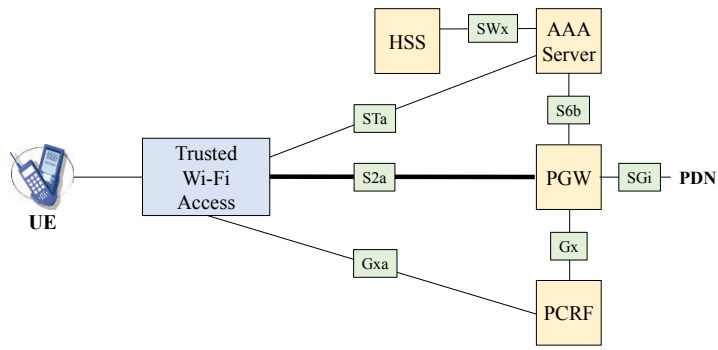

Figure 4.1. *Functional architecture based on the S2a interface*

The user profile is stored in the HSS entity for the establishment of the default bearers and, in this case, the presence of the PCRF is optional.

The presence of the PCRF entity is mandatory for the establishment of the dedicated bearers on the initiative of an application function (AF) whose first example of implementation is the VoLTE (Voice over LTE) that provides telephone service.

The characteristics of the dedicated bearer for the IP packet containing the voice are only stored in the SPR (Subscription Profile Repository) database associated with the PCRF entity.

A trusted WLAN access network (TWAN) includes the following features:

– WLAN AN: this feature includes Wi-Fi access points;

– TWAG (Trusted WLAN Access Gateway): this function terminates the S2a tunnel;

– TWAP (Trusted WLAN AAA Proxy): this function terminates the STa interface.

The transparent single-connection (TSC) mode provides a single connection to the PGW entity without the mobility support between LTE and Wi-Fi radio accesses. The IPv4 and/or IPv6 address of the mobile is provided by the TWAG function:

– in the case of a stateful configuration, the TWAG function acts as a DHCP (Dynamic Host Configuration Protocol) server;

– in the case of a stateless configuration, the TWAG function broadcasts the prefix of the IPv6 address.

The single-connection mode (SCM) supports the mobility between LTE and Wi-Fi accesses. This mode also supports non-seamless WLAN offload (NSWO) for which the traffic is directly routed to the Internet network through the TWAG function.

The multi-connection mode (MCM) supports NSWO and multi-access PDN connectivity (MAPCON) for which the various connections to the PDN pass through LTE (e.g. telephone service) or Wi-Fi (e.g. Internet service) interfaces according to the policy of the operator. The mobility between LTE and Wi-Fi radio accesses is possible. This mode also supports the NSWO function.

The connection via Wi-Fi interface is established by WLCP (WLAN Control Plane) protocol. The connection is identified by the MAC address of the mobile associated with a MAC address of the TWAG function.

For the single- or multi-connection modes, the IPv4 and/or IPv6 address of the mobile is provided by the PGW entity.

The PGW entity allocates the downlink packets to different S2a bearers based on the TFT (Traffic Flow Template) packet filters set up during the establishment of the S2a bearer (Figure 4.2).

The TWAN function of the trusted Wi-Fi access assigns the uplink packets to different S2a bearers based on the TFT packet filters set up during the establishment of the S2a bearer (Figure 4.2).

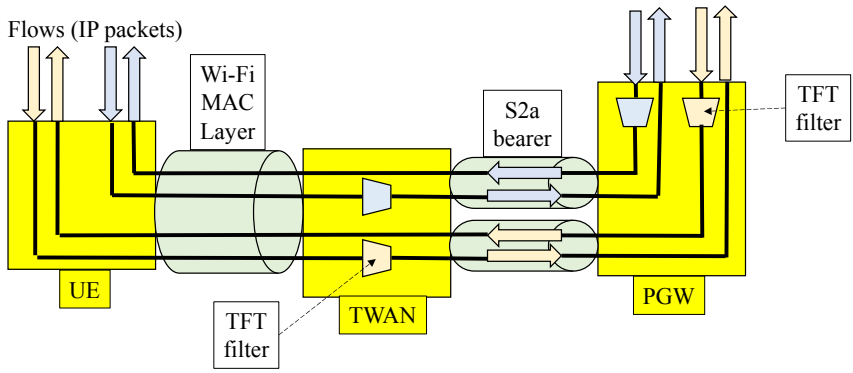

Figure 4.2. *Connection to the PDN for the architecture based on the S2a interface*

4.1.2. *Architecture based on the S2b interface*

The functional architecture based on the S2b interface corresponds to the untrusted Wi-Fi access and network-based mobility (Figure 4.3).

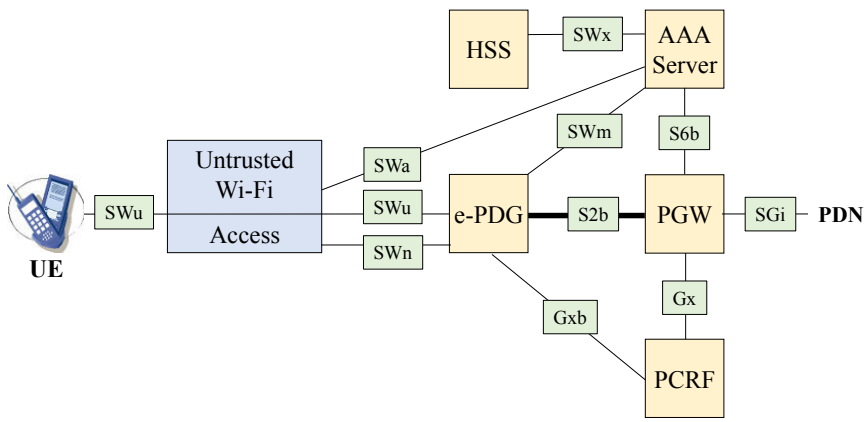

Figure 4.3. *Functional architecture based on the S2b interface*

The mobile stream passes through the SWu and S2b tunnels to access the PDN via the PGW entity. The SWu tunnel is built between the mobile and the evolved packet data gateway (ePDG). The S2b tunnel is built between the ePDG and PGW entities.

The HSS entity and the AAA server provide the following functions:

– mutual authentication of the mobile and the AAA server, via the SWx and SWa interfaces. This authentication has the effect of opening Wi-Fi access to the mobile;

– mutual authentication related to the establishment of the SWu tunnel, via the SWx and SWm interfaces;

– transfer of the mobile profile to the PGW entity via the interface S6b, the ePDG entity via the SWm interface and the untrusted Wi-Fi access via the SWa interface. The mobile profile contains a list of access point names (APN) and the quality of service (QoS) level of the S2b tunnel.

The PCRF entity provides the QoS level of the S2b tunnel to the PGW via the Gx interface and to the ePDG via the Gxb interface.

The PCRF entity provides the QoS level of the SWu tunnel to the ePDG entity via the Gxb interface. In this case, the ePDG entity provides the QoS level to be applied on the Wi-Fi radio interface via the SWn interface.

The mobile must establish an SWu instance for each PDN connection.

When the mobile connects to the PDN, a default bearer must be established on the S2b interface. This connection is maintained for the duration of the connection.

Dedicated bearers can be built for the same PDN connection, based on the rules provided by the PCRF.

A SWu instance transports the packets of all S2b bearers for the same connection to the PDN between the mobile and the ePDG entity.

The ePDG entity shall release the SWu instance when the S2b default bearer of the associated connection to the PDN is released.

Two IPv4 and/or IPv6 addresses are assigned to the mobile:

– an address for the SWu tunnel built between the mobile and the ePDG entity, provided by the untrusted Wi-Fi access;

– an address for the flow transiting in this tunnel, provided by the PGW entity.

The connection to the PDN is described in Figure 4.4.

The PGW entity must allocate the downlink packets to different S2b bearers according to the TFT packet filters set up during the establishment of the S2b bearer.

The ePDG entity must assign the downlink packets to the SWu instance based on the correspondence between the SWu instance and the identifier of the S2b bearer.

The mobile must assign the uplink packets to the SWu instance based on the correspondence between the APN identifier of the PDN connection and the SWu instance.

The ePDG entity must allocate uplink packets to different S2b bearers according to the TFT packet filters, which are set up during the establishment of the S2b bearer.

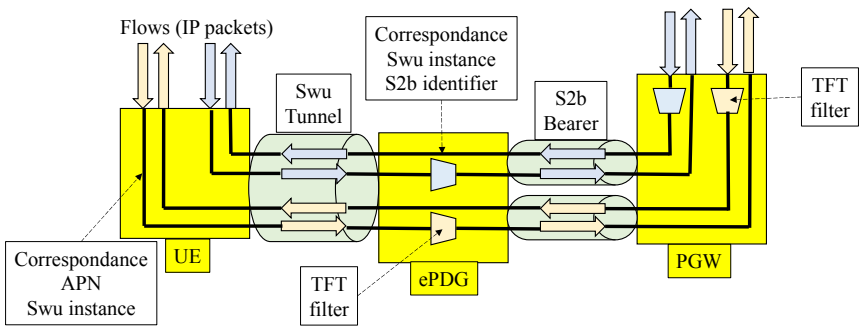

Figure 4.4. *Connection to the PDN for the architecture based on the S2b interface*

4.1.3. *Architecture based on the S2c interface*

The functional architecture based on the S2c interface corresponds to a mobility based on the mobile. The functional architecture is shown in Figure 4.5 for the trusted Wi-Fi access and Figure 4.6 for the untrusted Wi-Fi access.

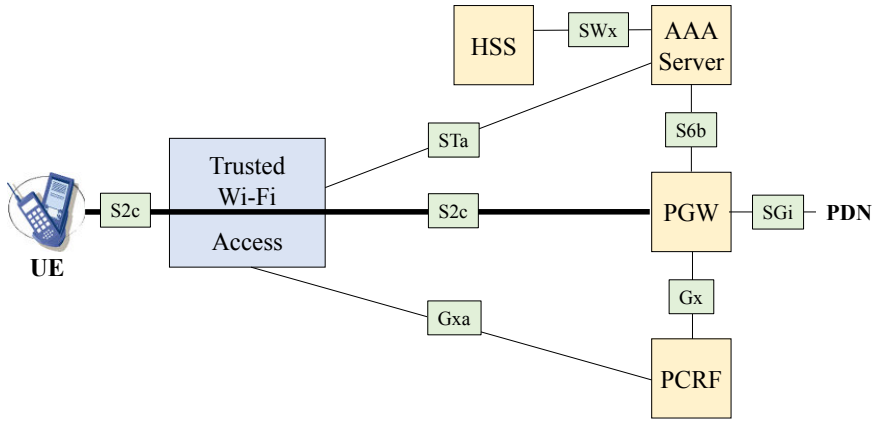

Figure 4.5. *Functional architecture based on the S2c interface trusted Wi-Fi access*

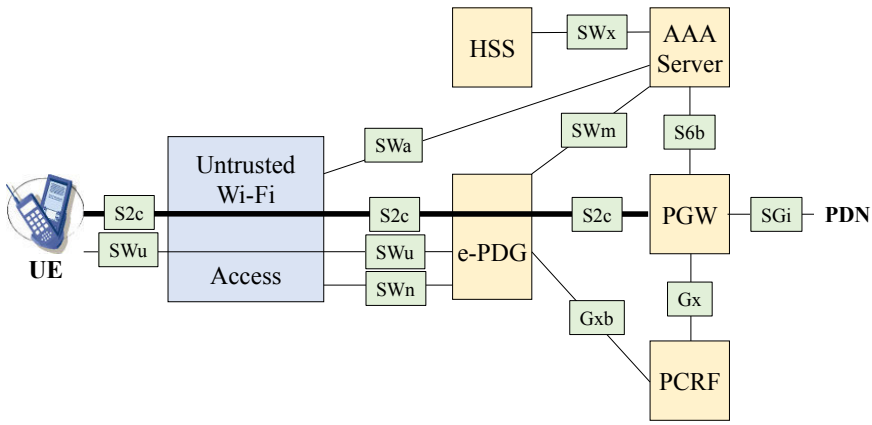

Figure 4.6. *Functional architecture based on the S2c interface untrusted Wi-Fi access*

The mobile data stream passes through the S2c tunnel built between the mobile and the PGW entity to access the PDN.

In the case of an untrusted Wi-Fi access, the S2c tunnel passes through the SWu tunnel built between the mobile and the ePDG entity.

4.2. Tunnel establishment

4.2.1. *Architecture based on the S2a interface*

The S2a interface is the point of reference between the PGW entity and the trusted Wi-Fi access. This interface supports several mechanisms for the establishment of the S2a tunnel.

The construction of the S2a tunnel requires the selection of the PGW entity by Wi-Fi access, according to information provided by the AAA server during authentication.

This information can be the IP address of the PGW entity, the full qualified domain name (FQDN) or the APN. The trusted Wi-Fi access retrieves the IP address of the PGW entity by performing DNS (Domain Name System) resolution based on the FQDN or the APN.

4.2.1.1. *PMIPv6 mechanism*

The PMIPv6 (Proxy Mobile IP version 6) mechanism relies on the signaling provided by the mobility extension of the IPv6 header exchanged between Wi-Fi access and the PGW entity (Figure 4.7) and on the GRE (Generic Routing Encapsulation) tunnel of the mobile data stream (Figure 4.8).

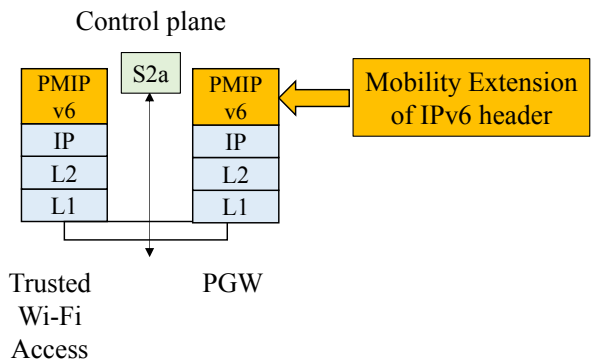

Figure 4.7. *Protocol architecture based on the S2a interface control plane for the PMIPv6 mechanism*

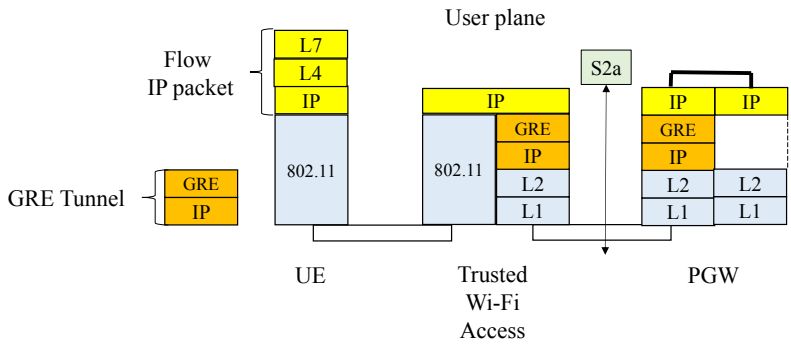

Figure 4.8. *Protocol architecture based on the S2a interface user plane for the PMIPv6 mechanism*

The MIPv6 mechanism requires functionality in the IPv6 stack of a mobile node. The exchange of signaling messages between the mobile node and the home network agent makes it possible to create and maintain a correspondence between its address in the home network and the foreign network.

Network-based mobility supports the mobility of IPv6 nodes without mobile involvement by extending MIPv6 signaling between the TWAG function and the PGW entity.

This approach to support mobility does not require the mobile node to be involved in the exchange of signaling messages. The PMIPv6 protocol is an extension of the MIPv6 protocol.

A mobile node can operate in an IPv4, IPv6 or IPv4/IPv6 environment. The PMIPv6 protocol independently supports the mobility of the IPv4 address and the transport of IP packets in an IPv4 network.

The PMIPv6 mechanism can transport IPv4 or IPv6 streams in IPv4 or IPv6 tunnels.

4.2.1.2. *MIPv4 mechanism*

The MIPv4 FA (Mobile IP version 4 Foreign Agent) mechanism is based on MIPv4 signaling (Figure 4.9) and the IP packet (the mobile data stream) encapsulated in the IP tunnel (Figure 4.10).

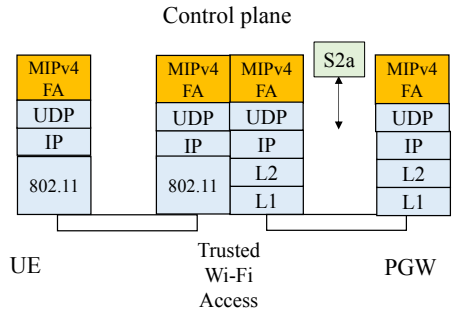

Figure 4.9. *Protocol architecture based on the S2a interface control plane for the MIPv4 FA mechanism*

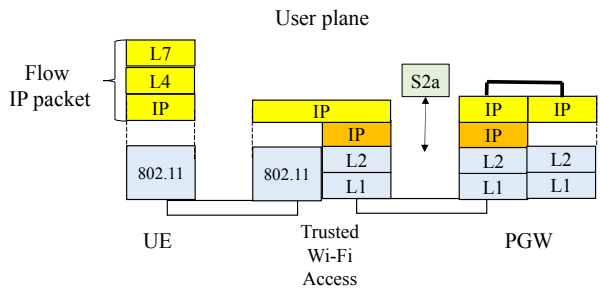

Figure 4.10. *Protocol architecture based on the S2a interface user plane for the MIPv4 FA mechanism*

MIPv4 signaling is exchanged, on the one hand, between the mobile and the trusted Wi-Fi access and, on the other hand, between the trusted Wi-Fi access and the PGW entity.

The MIPv4 protocol allows Wi-Fi access, playing the role of a foreign agent, to assign the mobile an IPv4 address in a foreign network.

The MIPv4 protocol makes it possible to register with the PGW entity, which plays the role of a home agent, the correspondence between the mobile IPv4 address in the home network, provided by the PGW entity, and the IPv4 address in the foreign network.

The MIPv4 mechanism makes it possible to transport only IPv4 streams in IPv4 tunnels.

4.2.1.3. *GTPv2 mechanism*

The GTPv2 (GPRS Tunneling Protocol version 2) mechanism is based on the GTPv2-C (Control) signaling exchanged between the trusted Wi-Fi access and the PGW entity (Figure 4.11) and on the GTP-U (User) tunnel of the mobile flow (Figure 4.12).

The GTPv2-C protocol allows the activation or the deactivation of a session as well as the creation, modification or release of GTP-U bearers.

The GTPv2 mechanism can transport IPv4 or IPv6 streams in IPv4 or IPv6 tunnels.

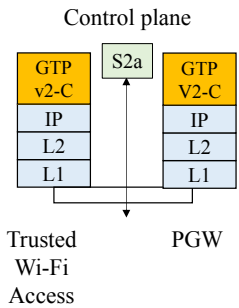

Figure 4.11. *Protocol architecture based on the S2a interface control plane for the GTPv2 mechanism*

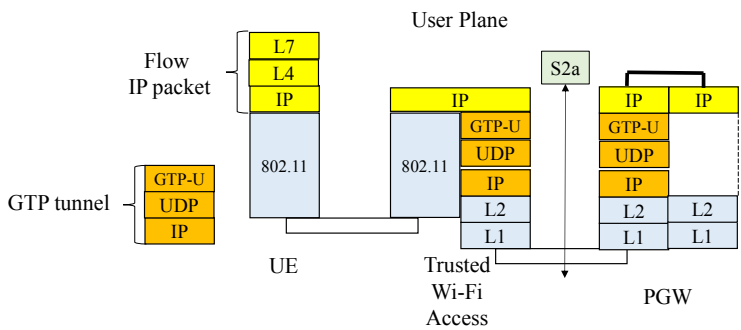

Figure 4.12. *Protocol architecture based on the S2a interface user plane for the GTPv2 mechanism*

4.2.2. *Architecture based on the S2b interface*

The S2b interface is the point of reference between the PGW and ePDG entities. This interface supports the PMIPv6 (Figures 4.13 and 4.14) or GTPv2 mechanisms for the establishment of the S2b tunnel.

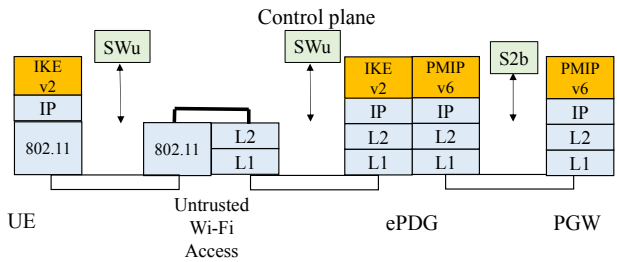

Figure 4.13. *Protocol architecture based on the S2b interface control plane for the PMIPv6 mechanism*

The SWu interface is the point of reference between the ePDG entity and the mobile. This interface supports the IPSec (IP Security) mechanism including IKEv2 (Internet Key Exchange version 2) signaling (Figure 4.13) and the ESP (Encapsulating Security Payload) tunnel of the mobile stream (Figure 4.14).

The construction of the SWu tunnel requires the retrieval of the IP address of the ePDG entity by the mobile. This IP address can be configured in the mobile by various means.

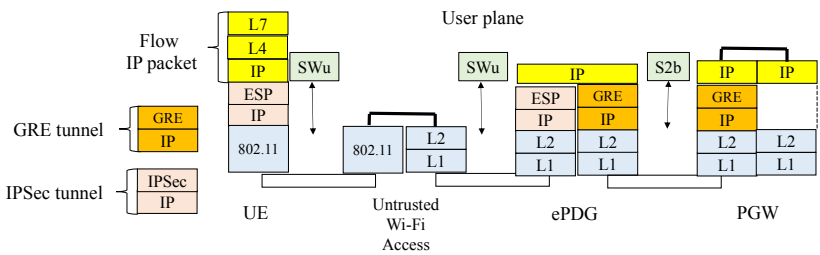

Figure 4.14. *Protocol architecture based on the S2b interface user plane for the PMIPv6 mechanism*

The mobile can also perform a DNS resolution on the FQDN of the ePDG entity. The mobile automatically builds the FQDN from the identity of the operator

contained in its international mobile subscriber identity (IMSI) or from the tracking area identify (TAI), where the mobile is located.

The construction of the S2b tunnel requires the selection of the PGW entity by the ePDG entity from information provided by the AAA server during the authentication for the establishment of the SWu tunnel.

4.2.3. *Architecture based on the S2c interface*

The S2c interface is the point of reference between the PGW entity and the mobile. This interface supports the DSMIPv6 (Dual-Stack Mobile IP version 6) mechanism for the establishment of the S2c tunnel built between the mobile and the PGW entity.

In the case of a trusted Wi-Fi access, this interface supports DSMIPv6 signaling (Figure 4.15) and IP in the IP tunnel (Figure 4.16) of the mobile stream.

In the case of an untrusted Wi-Fi access, the IPSec tunnel established between the mobile and the ePDG entity protects the S2c interface.

The MIPv6 protocol allows IPv6 mobile nodes to move while maintaining accessibility and ongoing sessions.

The DSMIPv6 protocol prevents the IPv4/IPv6 dual-stack mobile from running both MIPv4 and MIPv6 mobility protocols simultaneously.

The DSMIPv6 protocol also takes into account the case where the mobile moves in a private IPv4 network. The mobile node must be able to communicate with the PGW entity, which acts as a home agent, through a NAT (Network Address Translation) device.

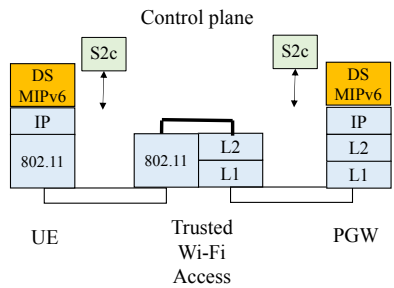

Figure 4.15. *Protocol architecture based on the S2c interface control plane for the trusted Wi-Fi access*

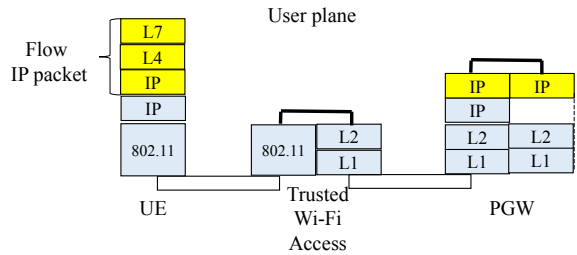

Figure 4.16. *Protocol architecture based on the S2c interface user plane for the trusted Wi-Fi access*

In the case of an untrusted Wi-Fi access, the S2c tunnel is established from the IP address of the PGW provided by the AAA server during the authentication for the establishment of the SWu tunnel.

The mobile can also retrieve the IP address of the PGW entity by querying a DHCP (Dynamic Host Configuration Protocol) server or by performing DNS resolution based on the FQDN of the PGW entity.

4.3. DIAMETER protocol

The DIAMETER protocol is used to perform authentication, authorization and accounting functions.

The authentication function makes it possible to control the access of the mobile to the 4G mobile network from a secret key stored, on the one hand, in the universal subscriber identity module (USIM) of the universal integrated circuit card (UICC) of the mobile and, on the other hand, in the HSS entity.

The authorization function retrieves the service and traffic profile of the mobile stored in the HSS and SPR databases.

The accounting function allows the generation of events from the PGW entity to the charging entities for the prepaid or postpaid service.

4.3.1. *AAA server interfaces*

The DIAMETER protocol is supported by the interfaces between, on the one hand, the AAA server, and on the other hand (Figure 4.17):

– the trusted Wi-Fi access via the STa interface;

– the untrusted Wi-Fi access via the SWa interface;

– the PGW entity via the S6b interface;

– ePDG entity via the SWm interface;

– the HSS entity via the SWx interface.

The SWx interface is used by the AAA server to retrieve the authentication data, the subscriber profile and the parameters for the PMIPv6, MIPv4 FA, GTPv2 and DSMIPv6 mechanisms.

The SWx interface is used to register the address of the PGW and the AAA server in the HSS when establishing tunnel S2a, S2b or S2c.

The SWx interface is used by the HSS entity for updating the mobile profile and for detaching it.

Table 4.1 summarizes the DIAMETER messages exchanged on the SWx interface.

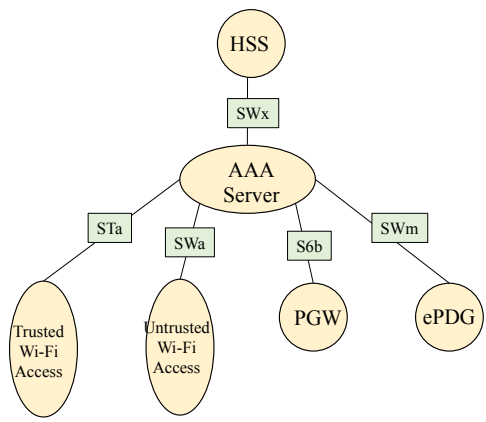

Figure 4.17. *AAA server interfaces using the DIAMETER protocol*

Messages	Comments
Multimedia-Authentication-Request (MAR)	AAA server request to retrieve authentication data
Multimedia-Authentication-Answer (MAA)	HSS entity response containing authentication data
Server-Assignment-Request (SAR)	AAA server request to register the PGW entity and retrieve the mobile profile
Server-Assignment-Answer (SAA)	HSS entity response containing mobile profile
Registration-Termination-Request (RTR)	HSS server request for mobile detachment
Registration-Termination-Answer (RTA)	AAA server response to RTR request
Push-Profile-Request (PPR)	HSS entity request for mobile profile update
Push-Profile-Answer (PPA)	AAA server response to PPR request

Table 4.1. *DIAMETER messages on the SWx interface*

The STa and SWa interfaces share the same authentication procedure. During the authentication phase, the AAA server decides whether Wi-Fi access is trusted or untrusted, and communicates the decision to the Wi-Fi access point.

The STa and SWa interfaces are used to carry information relating to the mechanisms PMIPv6, MIPv4 FA (only in the case of the STa interface), GTPv2 and DSMIPv6.

The STa and SWa interfaces are used for detaching the mobile, the procedure being at the initiative of the Wi-Fi access or the AAA server.

The STa and SWa interfaces are used to renew mobile authentication. The procedure is initiated by the AAA server in the event that the subscriber's profile stored in the HSS entity is changed, or at the initiative of the Wi-Fi access that wants to verify that the subscriber's profile is not modified.

Table 4.2 summarizes the DIAMETER messages exchanged on the STa and SWa interfaces.

Messages	Comments
Authenticate and Authorize Request (AAR)	Wi-Fi access request to register and retrieve the mobile profile
Authenticate and Authorize Answer (AAA)	AAA server response containing mobile profile
Re-Auth-Request (RAR)	AAA server request for mobile authentication renewal
Re-Auth-Answer (RAA)	Response from Wi-Fi access to RAR request
Session Termination Request (STR)	Wi-Fi access request for ending the mobile session
Session Termination Answer (STA)	AAA server response to STR
Abort-Session-Request (ASR)	AAA server request for termination of mobile session
Abort-Session-Answer (ASA)	Response from Wi-Fi access to ASR
Diameter-EAP-Request (DER)	Wi-Fi access request used for the EAP-AKA authentication procedure
Diameter-EAP-Answer (DEA)	AAA server response used for the EAP-AKA authentication procedure

Table 4.2. *DIAMETER messages on the STa and SWa interfaces*

The S6b interface is used by the PGW entity to communicate its address to the AAA server when the tunnel S2a, S2b or S2c is established.

The S6b interface is used by the PGW entity to retrieve the subscriber's profile and the PMIPv6 and GTPv2 mechanism information.

The S6b interface is used by the PGW entity to retrieve mobile authentication data for the DSMIPv6 mechanism. The authentication data is used to control the establishment of the IPSec mechanism to protect the DSMIPv6 signaling exchanged between the mobile and the PGW entity.

The S6b interface is used for terminating the mobile session, the procedure being initiated by the PGW entity or the AAA server.

Table 4.3 summarizes the DIAMETER messages exchanged on the S6b interface.

Messages	Comments
Authenticate and Authorize Request (AAR)	PGW entity request to register and retrieve the mobile profile
Authenticate and Authorize Answer (AAA)	AAA server response containing mobile profile
Re-Auth-Request (RAR)	AAA server request for mobile authentication renewal
Re-Auth-Answer (RAA)	PGW response to RAR
Session Termination Request (STR)	PGW request for termination of mobile session
Session Termination Answer (STA)	AAA server response to STR
Abort-Session-Request (ASR)	AAA server request for termination of mobile session
Abort-Session-Answer (ASA)	PGW response to ASR
Diameter-EAP-Request (DER)	Request of the PGW entity used for the EAP-AKA authentication procedure for the DSMIPv6 mechanism
Diameter-EAP-Answer (DEA)	AAA server response used for the EAP-AKA authentication procedure

Table 4.3. *DIAMETER messages on the S6b interface*

The SWm interface is used for the mutual authentication procedure of the mobile and the AAA server which is implemented during the establishment of the SWu tunnel.

The SWm interface is used by the ePDG entity to retrieve the subscriber's profile and the PMIPv6 and GTPv2 mechanism information.

The SWm interface can also be used to transmit to the ePDG entity the IP address or the FQDN of the PGW entity.

The SWm interface is used for terminating the mobile session, the procedure being initiated by the ePDG entity or the AAA server.

Table 4.4 summarizes the DIAMETER messages exchanged on the SWm interface.

Messages	Comments
Authenticate and Authorize Request (AAR)	Request from the ePDG entity to register itself and retrieve the mobile profile
Authenticate and Authorize Answer (AAA)	AAA server response containing mobile profile
Re-Auth-Request (RAR)	AAA server request for mobile authentication renewal
Re-Auth-Answer (RAA)	Response of the ePDG entity to the RAR
Session Termination Request (STR)	Request from ePDG entity for the termination of mobile session
Session Termination Answer (STA)	AAA server response to STR
Abort-Session-Request (ASR)	AAA server request for termination of mobile session
Abort-Session-Answer (ASA)	Response of the ePDG entity to the ASR
Diameter-EAP-Request (DER)	Request of the ePDG entity used for the EAP-AKA authentication procedure for the DSMIPv6 mechanism
Diameter-EAP-Answer (DEA)	AAA server response used for the EAP-AKA authentication procedure

Table 4.4. *DIAMETER messages on the SWm interface*

4.3.2. *PCRF interfaces*

The DIAMETER protocol is also supported on the interfaces between, on the one hand, the PCRF entity, and on the other hand (Figure 4.18):

– the PGW entity via the Gx interface;

– the trusted Wi-Fi access via the Gxa interface;

– the ePDG entity via the Gxb interface.

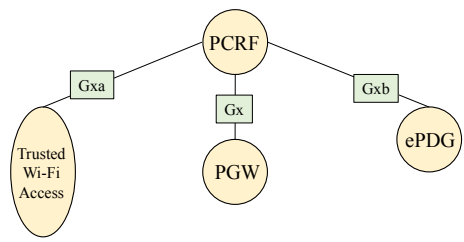

Figure 4.18. *PCRF interfaces using the DIAMETER protocol*

The Gx, Gxa and Gxb interfaces make it possible to request the PCRF entity:

– to retrieve the rules to apply to the default bearer created by the EPS network;

– to inform the PCRF entity of the termination of the session on the EPS network.

The Gx, Gxa and Gxb interfaces allow the PCRF entity to provide the rules to be applied for the dedicated bearer.

Table 4.5 summarizes the DIAMETER messages exchanged on the Gx, Gxa and Gxb interfaces.

Messages	Comments
Credit-Control-Request (CCR)	Request from PGW, ePDG or trusted Wi-Fi entities to retrieve the mobile profile
Credit-Control-Answer (CCA)	PCRF response containing the mobile profile
Re-Auth-Request (RAR)	Request from the PCRF entity containing the mobile profile
Re-Auth-Answer (RAA)	Response of PGW, ePDG or trusted Wi-Fi access to the RAR

Table 4.5. *DIAMETER messages on the Gx, Gxa and Gxb interfaces*

5

Wi-Fi Integration – Procedures

5.1. Mutual authentication

5.1.1. *EAP-AKA method*

The authentication and key agreement (AKA) mechanism allows mutual authentication and then the distribution of keys for data confidentiality and signaling data confidentiality and integrity, during the attachment of the mobile to the 4G mobile network.

Authentication is based on AUTN (Authentication Network) and RES (Result) seals generated by the home subscriber server (HSS) and the mobile from a RAND sequence and the secret key Ki.

The RAND sequence is generated by the HSS entity and then transmitted to the mobile. The secret key Ki is stored in the universal subscriber identity module (USIM) of the universal integrated circuit card (UICC) of the mobile and in the HSS entity during the creation of the subscription.

The integrity key (IK) and the cipher key (CK) are generated by the HSS entity and the mobile from a derivation of the Ki key using the RAND sequence. The pairwise master key (PMK) is derived from the keys CK and IK.

The EAP-AKA method is applied in the case of an untrusted Wi-Fi access when establishing the SWu tunnel.

In the case of a trusted Wi-Fi access, the EAP-AKA' method replaces the EAP-AKA method. The modification concerns the derivation of the keys CK and IK, which takes into account the identity of the access network and the derivation algorithm.

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

The three components involved in the authentication procedure are integrated into the following entities:

– the supplicant is represented by the mobile which wishes to access the 4G mobile network;

– the authenticator is represented by the trusted Wi-Fi access that controls the access of the supplicant to the 4G mobile network;

– the authentication server is represented by the AAA (Authentication, Authorization and Accounting) server, which authenticates the supplicant and authorizes access to the 4G mobile network.

The AKA' mechanism is implemented from extensible authentication protocol (EAP)-AKA' messages transported between the mobile and the trusted Wi-Fi access in EAPOL (EAP Over LAN) messages (Figure 5.1).

EAP-AKA' messages are carried between the trusted Wi-Fi access and the AAA server in DIAMETER messages:

– DER (Diameter-EAP-Request) message is transmitted by the trusted Wi-Fi access;

– DEA (Diameter-EAP-Answer) is transmitted by the AAA server.

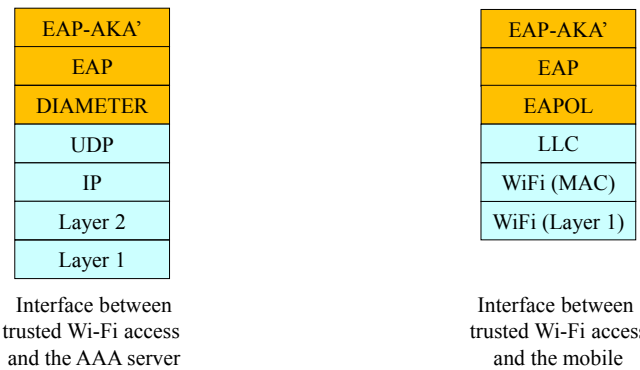

Figure 5.1. *Transport of the EAP-AKA' messages*

5.1.2. *Mutual authentication procedure*

The procedure of mutual authentication, in the case of a trusted Wi-Fi access, is part of the procedure of attachment of the mobile.

At the end of the association phase with the trusted Wi-Fi access, the mobile transmits the EAPOL-Start message, which triggers the mutual authentication procedure based on the EAP-AKA' method (Figure 5.2).

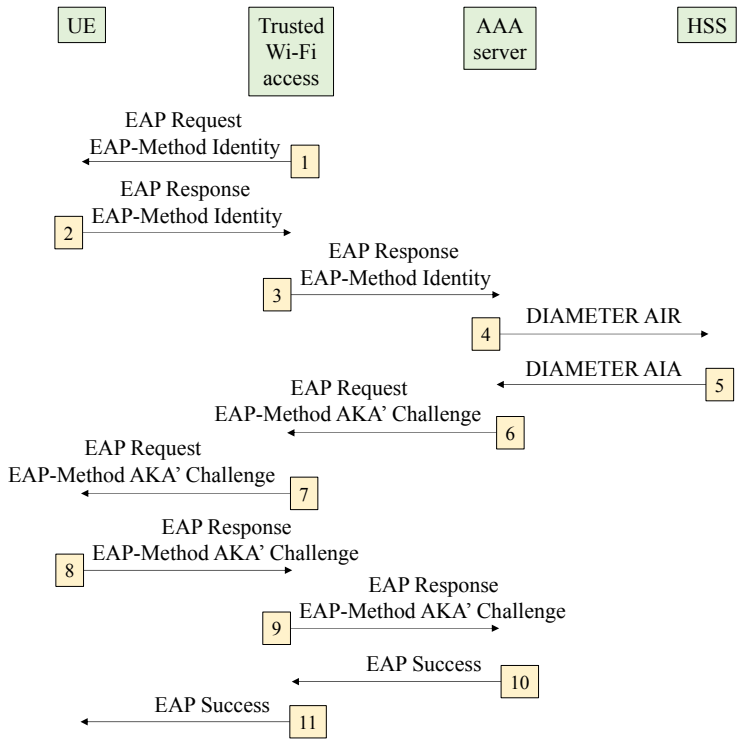

Figure 5.2. *Mutual authentication procedure*

1) Trusted Wi-Fi access sends the EAP Request message containing the EAP-Method Identity message.

2) The mobile transmits the EAP Response/EAP-Method Identity message containing, at the first authentication, the network access identifier (NAI) constructed from the international mobile subscriber identity (IMSI) of the mobile.

3) Wi-Fi access completes the EAP Response/EAP-Method Identity message, including the access network parameters (type, identity) and transfers it to the AAA server in a message DIAMETER DER.

4) The AAA server asks the HSS entity for the authentication vector of the mobile in the message DIAMETER AIR (Authentication-Information-Request).

The HSS entity generates a RAND sequence and creates the RES, AUTN, CK' and IK' parameters from the Ki key and the RAND sequence.

5) The HSS entity transmits the authentication vectors to the AAA server in the message DIAMETER AIA (Authentication-Information-Answer).

6) The AAA server derives two keys CK' and IK' to generate the master key PMK and generates a pseudonym and possibly an identifier for the rapid renewal of the authentication.

The pseudonym or the identifier is a temporary identity constructed from encryption of the private identity IMSI, using the advanced encryption standard (AES) algorithm. The same secret key is used by all AAA servers.

The AAA server transmits to the trusted Wi-Fi access the EAP Request/EAP-Method AKA' Challenge message containing the identity of the access network, the RAND sequence, the AUTN seal, the pseudonym and possibly the identifier for the renewal of the authentication.

This message is transmitted in a message DIAMETER DEA and contains a message authentication code (MAC) for the integrity check.

7) Trusted Wi-Fi access transfers the EAP Response/EAP-Method AKA' Challenge message to the mobile.

8) The mobile locally calculates, from its Ki key and the received RAND number, the PMK, its seal RES and the expected AUTN seal network. The mobile compares the received AUTN to the calculated value. If both values are the same, the network is authenticated. The mobile also controls the integrity of the received message.

The mobile transmits the EAP Response/EAP-Method AKA' Challenge message containing the RES seal and the MAC seal for the integrity check of the message to the trusted Wi-Fi access.

9) The trusted Wi-Fi access transfers the EAP Response/EAP-Method AKA' Challenge message to the AAA server in a message DIAMETER DER.

10) The AAA server checks the integrity of the received message and compares the RES seal received from the mobile to that received from the HSS entity. If the two values are identical, the mobile is authenticated.

The AAA server transmits the message DIAMETER DEA containing the EAP Success message and the PMK to the trusted Wi-Fi access.

11) The trusted Wi-Fi access stores the PMK and transfers the EAP Success message to the mobile.

5.1.3. *Procedure for rapid renewal of authentication*

The rapid renewal of authentication makes it possible to avoid repeating the procedure from the authentication vector (RAND, AUTN, RES, CK', IK').

The implementation of the procedure for rapid renewal of authentication is indicated by the AAA server, during the initial authentication procedure, when it supplies the corresponding identifier.

The identity of the access network must not change during the procedure for rapid renewal of authentication. If this happens, the normal authentication procedure must be carried out.

The procedure for rapid renewal of the authentication is described in Figure 5.3.

Steps 1 to 3 are identical to those described for initial authentication in Figure 5.2. The private identity used by the mobile is the identifier for rapid renewal of authentication.

4) The AAA server transmits to the trusted Wi-Fi access the EAP Request/EAP-Method AKA' Reauthentication message containing a random number (nonce) for the generation of a new PMK and a new identifier for the next authentication.

This message is transmitted in a message DIAMETER DER and contains a MAC seal for the integrity check.

5) The trusted Wi-Fi access transfers the EAP Response/EAP-Method AKA' Reauthentication message to the mobile.

6) The mobile checks the integrity of the received message and acknowledges it in the EAP Response/EAP-Method AKA' Reauthentication message containing a MAC seal.

7) The trusted Wi-Fi access transfers the EAP Response/EAP-Method AKA' Reauthentication message to the AAA server in a message DIAMETER DER.

Steps 8 and 9 are identical to those described for initial authentication in Figure 5.2.

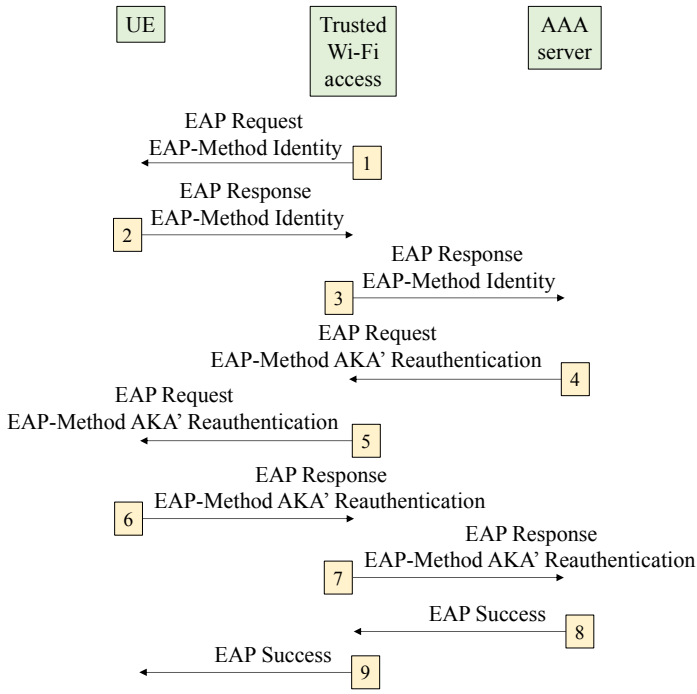

Figure 5.3. *Procedure for rapid renewal of authentication*

5.1.4. *Application to the MIPv4 FA mechanism*

The MIPv4 FA (Mobile IP version 4 Foreign Agent) mechanism is an alternative for building the S2a tunnel containing the mobile stream.

The MIPv4 FA mechanism defines the following three components:

– the mobile node (MN) component integrated into the mobile;

– the home agent (HA) component integrated into the PDN Gateway (PGW);

– the foreign agent (FA) component integrated into an entity (e.g. a router) of the Wi-Fi access network, which is not necessarily the trusted Wi-Fi access.

During the mutual authentication procedure, the AAA server and the mobile also generate the extended master session key (EMSK) from the CK' and IK'.

Two keys MN-HA and MN-FA are generated from the EMSK to protect the MIPv4 messages exchanged between, on the one hand, the component MN and, on the other hand, the components HA and FA.

1) The AAA server and the mobile derive the EMSK to generate the MIP-RK (Mobile IP Root Key).

2) The AAA server and the mobile derive the MIP-RK to generate the FA-RK. The AAA server transfers the FA-RK to the trusted Wi-Fi access.

3) The AAA server and the mobile derive the MIP-RK to generate the MN-HA key. The AAA server transfers the MN-HA key to the PGW entity.

4) The mobile and the trusted Wi-Fi access derive the FA-RK to generate the MN-FA key. The trusted Wi-Fi access transfers the MN-FA key to the FA component.

5.2. SWu tunnel establishment

5.2.1. *IPSec mechanism*

The SWu tunnel establishment uses the IPSec (Internet Protocol Security) mechanism, which offers security services (authentication, integrity and confidentiality) in an identical way in IPv4 and IPv6. Their implementation is optional in IPv4 but mandatory in IPv6. Their use is optional.

Security services are offered through the use of AH (Authentication Header) or ESP (Encapsulating Security Payload) extensions of the IPv4 or IPv6 header.

The authentication header (AH) is designed to ensure the integrity and authentication of IP packets without data encryption (no confidentiality).

The encapsulating security payload (ESP) ensures the integrity, authentication and confidentiality of IP packets.

To secure a two-directional communication between two end points, a security association (SA) pair is required. The IKE (Internet Key Exchange) protocol dynamically ensures the creation of the security association.

A security association contains the following parameters:

– the authentication algorithm and the key in order to generate the AH extension;

– the encryption algorithm and the key in order to generate the ESP extension;

– the authentication algorithm and the key in order to generate the ESP extension, if this service is used;

– the lifetime of the security association;

– the encapsulation mode (tunnel or transport).

5.2.2. *SWu tunnel establishment procedure*

The procedure for establishing the SWu tunnel takes place between the mobile acting as the initiator and the evolved packet data gateway (ePDG) as the responder (Figure 5.4).

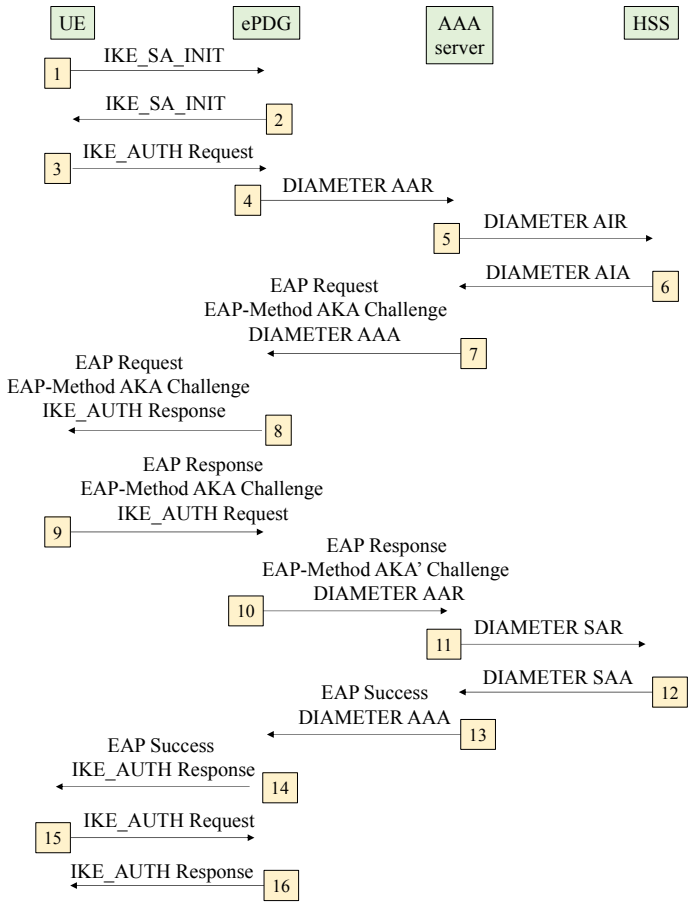

Figure 5.4. *SWu tunnel establishment procedure*

1) and 2) The two IKE_SA_INIT messages are used to negotiate the IKEv2 security association algorithms, and to exchange D–H public values and random numbers (nonce).

3) The mobile transmits the first message Request of the IKE_AUTH phase containing SWu tunnel configuration proposals in the SA block, its identity in the IDi block and access point name (APN) information in the IDr block.

The mobile does not transmit the AUTH block in order to warn the ePDG entity that it wishes to use the IKEv2 message to transport the EAP-AKA method.

The identity of the mobile conforms to the network access identifier (NAI) format containing the international mobile subscriber identity (IMSI) during the first authentication, or, during the following authentications, a pseudonym or an identifier for the rapid renewal of authentication.

The mobile transmits the CP block (CFG_REQUEST) in the IKE_AUTH Request message to obtain its IPv4 and/or IPv6 address, and possibly the IP address of the PGW entity, in the case where the mobility is managed by the mobile.

4) The ePDG entity transmits to the AAA server the message DIAMETER AAR (Authentication-Authorization-Request) containing the identity of the mobile and the information relating to the APN.

NAI analysis allows the AAA server to distinguish between either authentication for the trusted Wi-Fi access based on the EAP-AKA' mechanism or authentication for the untrusted Wi-Fi access based on the AKA mechanism.

5) The AAA server requests the home subscriber server (HSS) for mobile authentication vector in the message DIAMETER AIR (Authentication-Information-Request).

The HSS entity generates the RAND sequence and creates the seals (RES, AUTN) and the keys (CK and IK) from the Ki key and the RAND sequence.

6) The HSS entity passes the authentication vectors to the AAA server in the message DIAMETER AIA (Authentication-Information-Answer).

The AAA server derives the CK and IK to generate the master session key (MSK).

7) The AAA server initiates the authentication procedure with the message EAP Request/EAP-Method AKA Challenge containing the AUTN and RAND

parameters. This message is transmitted in the message DIAMETER AAA (Authentication-Authorization-Answer).

8) The ePDG entity transfers the message EAP Request/EAP-Method AKA Challenge in the message IKE_AUTH Response containing its identity, certificate and signature.

The mobile verifies the signature of the message IKE_AUTH Response with the public key of the ePDG entity retrieved from its certificate.

The mobile generates the RES, AUTN, CK and IK parameters from the Ki key and the received RAND sequence and compares the received AUTN seal to the locally calculated one. If both seals are identical, the AAA server is authenticated.

The mobile derives both CK and IK to generate the master key (MSK).

9) The mobile transmits the message EAP Response/EAP-Method AKA Challenge containing the RES seal in the message IKE_AUTH Request.

10) The ePDG entity transfers the message EAP Response/EAP-Method AKA Challenge in the message DIAMETER AAR to the AAA server which compares the received RES seals respectively from the mobile and the HSS entity. If the two seals are identical, then the mobile is authenticated.

11) The AAA server transmits the message DIAMETER SAR (Server-Assignment-Request) to the HSS entity to register itself.

12) The HSS entity responds to the AAA server with the message DIAMETER SAA (Server-Assignment-Answer) containing the subscriber's profile. The AAA server verifies that Wi-Fi access is allowed.

13) The AAA server transmits to the ePDG entity the message DIAMETER AAA containing the EAP Success message, the MSK and the subscriber's profile.

14) The ePDG entity stores the MSK and forwards the EAP Success message into the message IKE_AUTH Response.

15) The mobile generates the message IKE_AUTH Request containing in the AUTH block a seal calculated from its MSK. This seal allows the authentication of the first message IKE_SA_INIT.

16) The ePDG entity checks the seal and starts the S2b tunnel setup procedure described in section 5.3.

The ePDG entity responds with the message IKE_AUTH Response containing in the AUTH block a seal calculated from its MSK, which enables authentication of the second message IKE_SA_INIT.

The message IKE_AUTH Response is also used to transfer to the mobile its configuration in the CP block (CFG_REPLY) and the final configuration of the SWu tunnel in the SA block.

The mobile configuration was received from the PGW when establishing the S2b tunnel described in section 5.3.

5.2.3. *Procedure for rapid renewal of authentication*

The procedure for rapid renewal of authentication is described in Figure 5.5.

Steps 1 to 4 are identical to those described for the establishment of the SWu tunnel in Figure 5.4.

The identifier for rapid renewal of authentication is transmitted in the IDi block of the first message IKE_AUTH Request.

5) The AAA server initiates the procedure for rapid renewal of authentication with the message EAP Request/EAP-Method AKA Reauthentication.

6) The ePDG entity transmits the message IKE_AUTH Response containing its identity, its certificate and the signature of the IKE_SA_INIT message in the AUTH block.

The message AKA Reauthentication EAP Request/EAP-Method is included to start the EAP procedure on IKEv2.

7) The mobile verifies the signature and responds with the message IKE_AUTH Request and the message EAP Response/EAP-Method Reauthentication containing the mobile seal.

8) The ePDG entity transfers the message EAP Response/EAP-Method Reauthentication to the AAA server.

Steps 9 to 12 are identical to steps 13 to 16 described for the establishment of the SWu tunnel in Figure 5.4.

The new MSK is generated by the AAA server and passed to the ePDG entity and the mobile. This new key is used to authenticate the first two IKE_SA_INIT messages.

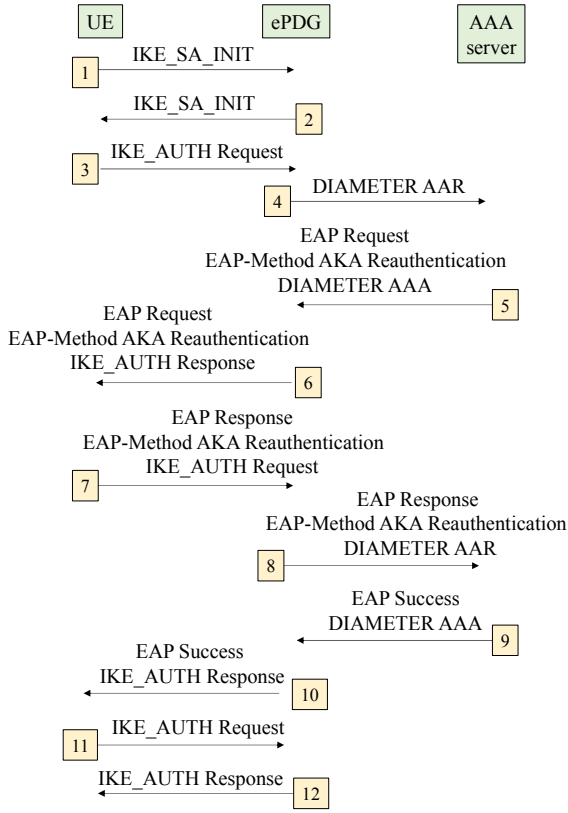

Figure 5.5. *Procedure for rapid renewal of authentication*

5.3. S2a/S2b tunnel establishment

5.3.1. *PMIPv6 mechanism*

The PMIPv6 (Proxy Mobile Internet Protocol version 6) mechanism allows a mobile host to keep its original IPv6 address, to maintain its current session or to be reachable when moving, mobility being provided by the network.

The mobile node (MN) is a host that changes network while retaining the home address (HoA) provided by its home network (Figure 5.6).

The mobile access gateway (MAG) is integrated into gateway router of the mobile node and provides mobility management for the mobile node connected to its local network (Figure 5.6).

The local mobility anchor (LMA) is built into the router that acts as the home agent (HA) of the mobile node and represents the anchor point for the mobile node (Figure 5.6).

In the case of auto-configuration, the LMA function provides the mobile node with an IPv6 home network prefix (HNP) from which the mobile node builds its HoA.

If not, the MAG function hosts a DHCPv6 server that assigns the HoA to the mobile, built from the IPv6 HNP.

The LMA function registers in the BCE (Binding Cache Entry) table the identity MN-ID of the mobile and the proxy care of address (CoA) of the MAG of the mobile node.

The tunnel built between the MAG and LMA functions is characterized by the proxy-CoA on the MAG side and the LMA address (LMAA) on the LMA side.

The local mobility domain (LMD) is a set consisting of an LMA function and several MAG functions attached to the LMA function (Figure 5.6).

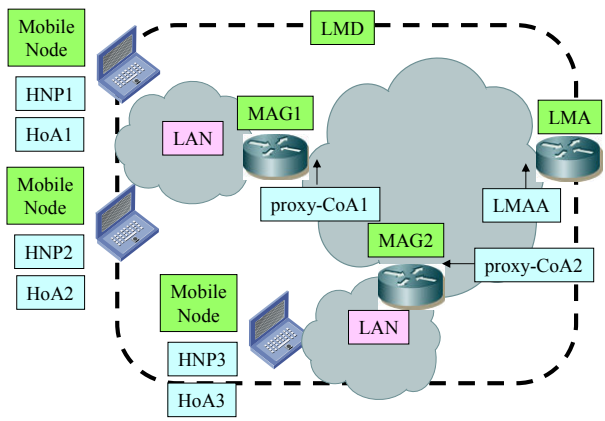

Figure 5.6. *PMIPv6 architecture*

5.3.1.1. *Trusted Wi-Fi access*

The LMA and MAG functions are hosted respectively by the PGW entity and the trusted Wi-Fi access.

The GRE (Generic Routing Encapsulation) protocol constructs the S2a tunnel from a key provided by the trusted Wi-Fi access for the downstream traffic and a key provided by the PGW for the traffic in the upstream direction.

The procedure for establishing the S2a tunnel is described in Figure 5.7 and corresponds to the auto-configuration of the IPv6 address by the mobile.

The procedure for S2a tunnel establishment starts when the mobile authentication, described in section 5.1, is successful.

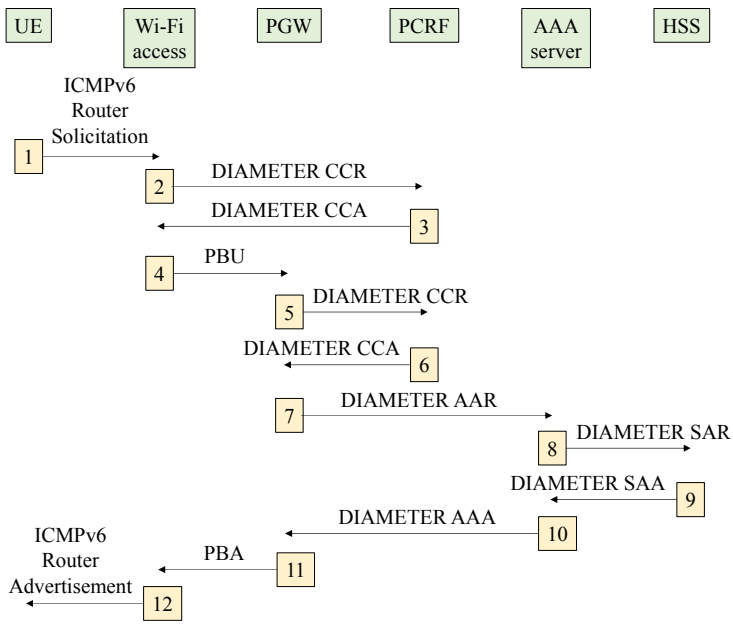

Figure 5.7. *S2a tunnel establishment using the PMIPv6 mechanism*

1) The mobile passes on the ICMPv6 message Router Solicitation to retrieve its IPv6 address configuration.

This message may contain the access point name (APN) that allows Wi-Fi access to determine the IP address of the PGW.

Otherwise, Wi-Fi access uses the default access point name that is passed by the AAA server during mobile authentication.

2) The Wi-Fi access transmits to the PCRF entity the message DIAMETER CCR (Credit-Control-Request) containing the subscriber's profile received from the AAA server during the authentication, to obtain the authorization for the opening of the default bearer.

The PCRF compares with the rules defined for the network and stored in the SPR (Subscription Profile Repository) database.

3) The PCRF responds to Wi-Fi access with the message DIAMETER CCA (Credit-Control-Answer) containing the rules to apply to the default bearer.

4) Wi-Fi access transmits to the PGW entity the PBU extension containing the following parameters: MN-NAI, Lifetime, Access Technology Type, APN, GRE key for downlink traffic, Charging Characteristics and Additional Parameters.

5) The PGW entity sends the PCRF entity the message DIAMETER CCR to obtain the default bearer characteristics.

6) The PCRF entity responds to the PGW entity with the message DIAMETER CCA containing the rules to apply to the default bearer (filter parameters, charging mode).

7) The PGW entity sends the AAA server the message DIAMETER AAR (Authentication-Authorization-Request) to communicate its identity and the access point name for the connection.

8) The AAA server sends the HSS entity the message DIAMETER SAR (Server-Assignment-Request) to transfer the information received from the PGW entity.

9) The HSS entity responds to the AAA server with the message DIAMETER SAA (Server-Assignment-Answer) that contains the subscriber's profile:

– the access point names (APN);

– QoS (Quality of Service) characteristics for each default bearer to be established.

10) The AAA server responds to the PGW entity with the message DIAMETER AAA (Authentication-Authorization-Answer) containing the information received from the HSS entity.

The PGW will use the subscriber's profile received from the AAA server if these parameters were not provided by the PCRF.

11) The PGW entity responds to the Wi-Fi access point with the PBA extension containing the following parameters: MN-NAI, Lifetime, UE Address Info, GRE key for uplink traffic, Charging ID and Additional Parameters.

12) Wi-Fi access responds to the mobile with the ICMPv6 message Router Advertisement containing the mobile configuration parameters (IPv6 prefix, IP address of the DNS server).

5.3.1.2. *Untrusted Wi-Fi access*

The LMA and MAG functions are hosted by the PGW and ePDG entities respectively.

The GRE protocol constructs the S2b tunnel from a key provided by the ePDG entity for downstream traffic and a key provided by the PGW entity for upstream traffic.

The procedure for establishing the S2b tunnel starts during the SWu tunnel establishment procedure described in section 5.2 (Figure 5.8).

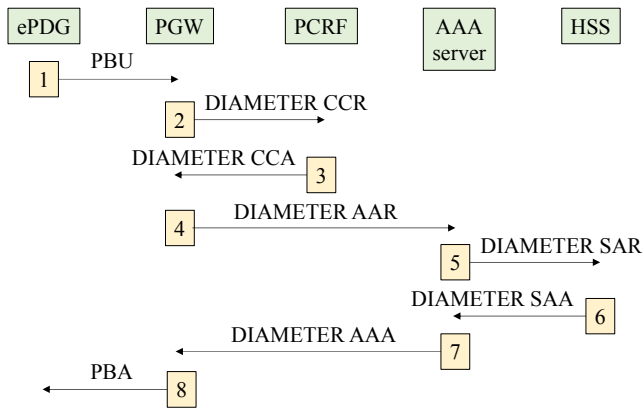

Figure 5.8. *S2b tunnel establishment using PMIPv6 mechanism*

1) The ePDG entity transmits to the PGW entity the PBU extension containing the following fields: MN-NAI, Lifetime, APN, Access Technology Type, GRE key for downlink traffic, UE Address Info, Charging Characteristics and Additional Parameters.

2) The PGW entity sends the PCRF entity the message DIAMETER CCR to obtain the mobile traffic profile.

3) The PCRF entity responds to the PGW entity with the message DIAMETER CCA containing the rules to be applied to the default bearer (APN-AMBR rate parameters and QoS).

4) The PGW entity sends the AAA server the message DIAMETER AAR to communicate its identity and the access point name for the connection.

5) The AAA server transmits to the HSS entity the message DIAMETER SAR to transfer the information received from the PGW entity.

6) The HSS entity responds to the AAA server with the message DIAMETER SAA to transfer the information received from the PGW entity.

7) The AAA server responds to the PGW entity with the message DIAMETER AAA containing the information received from the HSS entity. The subscriber's profile is taken into account if the PCRF did not provide the information in step 3.

8) The PGW entity responds to the ePDG entity with the PBA extension containing the following fields: MN-NAI, UE Address Info, GRE Key for uplink traffic and Charging ID.

The ePDG entity completes the SWu tunnel establishment procedure described in section 5.2.

5.3.2. *GTPv2 mechanism*

The GTPv2 (GPRS Tunneling Protocol version 2) mechanism comprises the GTPv2-C (Control) signaling that manages the S2a or S2b tunnel and the GTP-U (User) protocol for building the S2a or S2b tunnel.

The GTPv2-C protocol allows the establishment or closure of the mobile context and the bearers of the mobile streams.

The tunnel is identified by the Tunnel Endpoint Identifier (TEID) carried by the GTP-U protocol, tunnel end IP addresses and UDP port numbers. The entity receiving the traffic data determines the value of the TEID parameter that the sending entity is to use.

5.3.2.1. *Trusted Wi-Fi access*

The GTP-U protocol constructs the S2a tunnel from a TEID provided by the trusted Wi-Fi access for the downstream traffic and a TEID provided by the PGW entity for the upstream traffic.

The S2a Tunneling procedure, shown in Figure 5.9, starts during the mutual authentication procedure between the mobile and AAA server detailed in section 5.1.

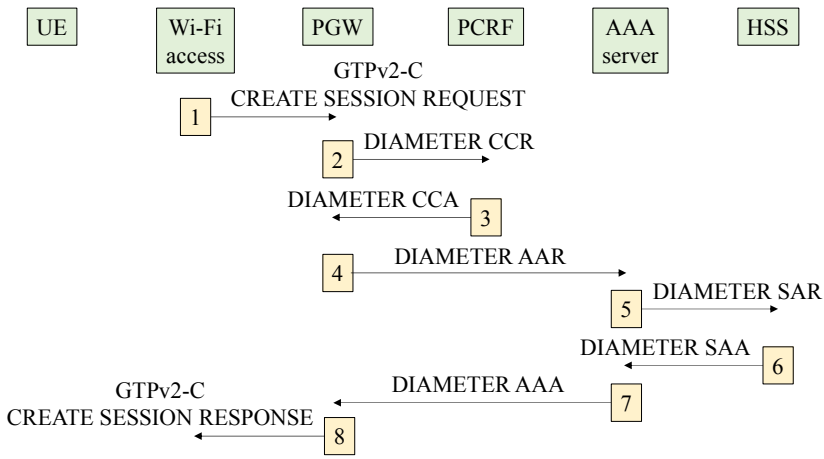

Figure 5.9. *S2a tunnel establishment using the GTPv2 mechanism*

1) The Wi-Fi access transmits to the PGW entity the GTPv2C message CREATE SESSION REQUEST containing the following fields: IMSI, APN, RAT type, PDN Type, PDN Address, Bearer Identity EPS, Default EPS QoS Bearer, AP Address, AP TEID, APN-AMBR, Charging Characteristics and Additional Parameters.

2) The PGW entity sends the PCRF entity the message DIAMETER CCR to obtain the default bearer characteristics. The PCRF entity can change the value of the APN-AMBR.

3) The PCRF entity responds to the PGW entity with the message DIAMETER CCA containing the rules to be applied to the default bearer (QoS parameters, filter parameters, charging mode).

4) The PGW entity sends the AAA server the message DIAMETER AAR to communicate its identity and the access point name for the connection.

5) The AAA server transmits to the HSS entity the message DIAMETER SAR to transfer the information received from the PGW entity.

6) The HSS entity responds to the AAA server with the message DIAMETER SAA.

7) The AAA server responds to the PGW entity with the message DIAMETER AAA.

8) The PGW entity responds to the trusted Wi-Fi access with the GTPv2C message CREATE SESSION RESPONSE, containing the following fields: PGW Address, PGW TEID, PDN Type, PDN Address, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR and Additional Parameters.

The trusted Wi-Fi access completes the authentication procedure (EAP Success message) by providing the elements of its configuration contained in the Additional Parameters field.

5.3.2.2. *Untrusted Wi-Fi access*

The GTP-U protocol constructs the S2b tunnel from a TEID provided by the ePDG entity for downstream traffic and a TEID provided by the PGW entity for upstream traffic.

The procedure for setting the S2a bearer resumes that described for the PMIPv6 mechanism with the following modifications:

The PBU message in step 1 is replaced by the CREATE SESSION REQUEST message containing the following fields: IMSI, APN, RAT type, TEID ePDG, PDN Type, PDN Address, Bearer Identity EPS, EPS QoS Bearer, ePDG Address, APN-AMBR and Additional Parameters.

The PBA message in step 8 is replaced by the CREATE SESSION RESPONSE message containing the following fields: PDN GW Address, PDN GW TEID, PDN Type, PDN Address, Bearer Identity EPS, EPS Bearer QoS, APN-AMBR and Charging ID.

5.3.3. *MIPv4 FA mechanism*

The mobile node is a host that changes network while retaining the HoA of its home network. When attached to a foreign network, it acquires an additional CoA (Figure 5.10).

The home agent (HA) is the entity of the originating network to which the mobile node must register when it attaches to a foreign network. The role of the home agent is to intercept the received packets and send them back in a tunnel to the mobile node. The HAA is that of the home agent interface on the home network of the mobile node (Figure 5.10).

The foreign agent (FA) is the entity of the network visited by the mobile node. It ends the tunnel and delivers the packets to the mobile node. The foreign agent address (FAA) is the gateway address of the mobile node in the visited network (Figure 5.10).

The correspondent node (CN) is the host that exchanges packets with the mobile node. Its address is denoted CNA (Correspondent Node Address) (Figure 5.10).

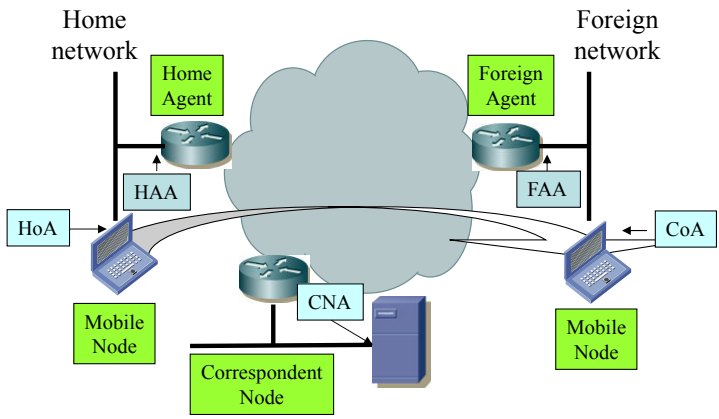

Figure 5.10. *Components of mobility*

The home agent (HA) and foreign agent (FA) functions are hosted respectively by the PGW entity and the trusted Wi-Fi access.

The trusted Wi-Fi access transfers the Registration Reply message to the mobile that retrieves its HoA address.

The procedure for setting up the S2a tunnel, described in Figure 5.11, starts after the mutual authentication procedure for the mobile and the AAA server detailed in section 5.1.

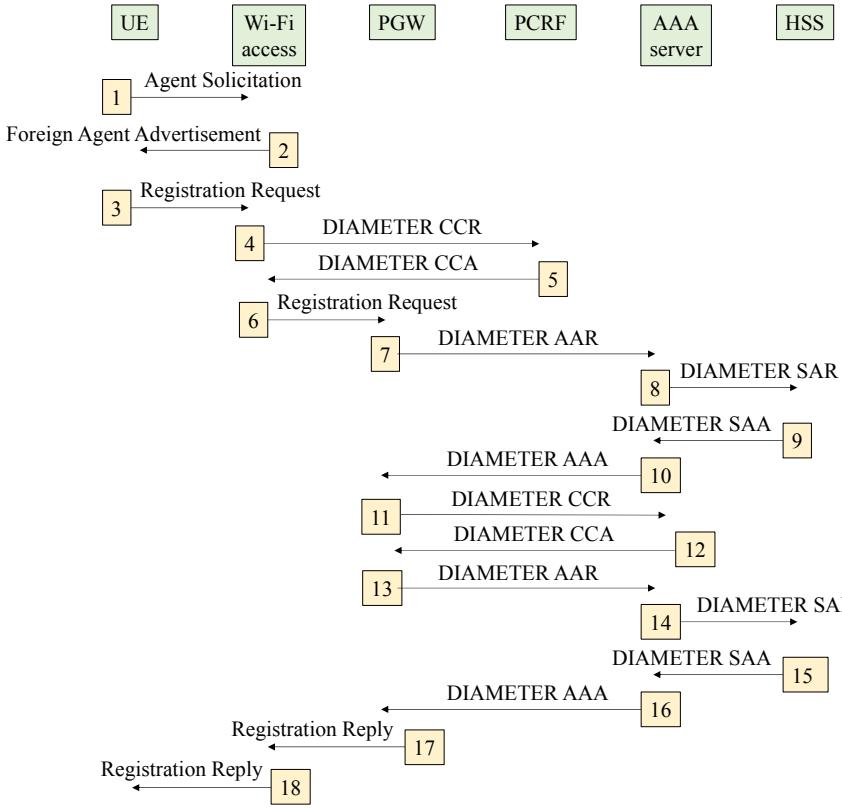

Figure 5.11. *S2a tunnel establishment using the MIPv4 FA mechanism*

1) The mobile transmits the ICMPv4 message Agent Solicitation.

2) Wi-Fi access responds to the mobile with the ICMPv4 message Foreign Agent Advertisement, containing the CoA of the foreign agent.

3) The mobile transmits the Registration Request message containing the following fields: MN-NAI, Lifetime and APN.

4) Wi-Fi access sends the PCRF entity the message DIAMETER CCR containing the subscriber's profile received from the AAA server during authentication, to obtain authorization to open the default bearer.

The PCRF may modify the received parameters if the rules defined for the network and stored in the SPR database are different.

5) The PCRF responds to Wi-Fi access with the message DIAMETER CCA containing the rules to apply to the default bearer.

6) Trusted Wi-Fi access transfers the Registration Request message to the PGW entity.

7) The PGW entity sends the message DIAMETER AAR to the AAA server to retrieve the subscriber's profile.

8) The AAA server transmits the message DIAMETER SAR to the HSS entity to retrieve the profile of the mobile.

9) The HSS entity responds to the AAA server with the message DIAMETER SAA containing the subscriber's profile.

10) The AAA server transmits to the PGW entity the message DIAMETER AAA containing the profile of the mobile.

11) The PGW entity sends the PCRF entity the message DIAMETER CCR to obtain the default bearer characteristics. The PCRF can change the value of the aggregate maximum bearer rate (APN-AMBR).

12) The PCRF entity responds to the PGW entity with the message DIAMETER CCA containing the rules to be applied to the default bearer (QoS parameters, filter parameters, charging mode).

13) The PGW entity sends the AAA server the message DIAMETER AAR to communicate its identity and the access point name for the connection.

14) The AAA server transmits to the HSS entity the message DIAMETER SAR to transfer the information received from the PGW.

15) The HSS entity responds to the AAA server with the message DIAMETER SAA.

16) The AAA server responds to the PGW entity with the message DIAMETER AAA.

17) The PGW entity responds to the trusted Wi-Fi access with the Registration Reply message containing the following fields: MN-NAI, Home Address (HoA), Home Agent Address (HAA) and Lifetime.

18) The trusted Wi-Fi access transfers the Registration Reply message to the mobile that retrieves its HoA.

5.4. S2c tunnel establishment

IPv6 mobility implements packet routing optimization between the mobile node and the correspondent node. The systematic routing of the packets exchanged via the home agent is simple to implement. On the other hand, if the mobile node is moving away from its home network and communicating with a correspondent node close to it, then it is more efficient to communicate directly rather than through the home agent.

The MIPv6 (Mobile IP version 6) mechanism was designed for a mobile connection to an IPv6 network. The DSMIPv6 (Dual-Stack Mobile IP version 6) mechanism also takes into account the connection of the mobile to a public or private IPv4 network. This arrangement makes it possible to avoid unrolling the two MIPv4 and MIPv6 mechanisms when the mobile has a dual IPv4 and IPv6 stack.

Several types of tunnel can be built between the mobile and the PGW entity that hosts the home agent functions:

– an IPv6 packet can be encapsulated by an IPv6 header;

– an IPv6 packet can be encapsulated by an IPv4 header. When the mobile is connected to an IPv4 private network, the tunnel must insert a UDP header between the IPv6 and IPv4 headers for traversal of the NAT (Network Address Translation) device;

– an IPv4 packet can be encapsulated by an IPv6 header;

– an IPv4 packet can be encapsulated by an IPv4 header. When the mobile is connected to an IPv4 private network, the tunnel must insert a UDP header between the two IPv4 headers for traversal of the NAT device.

The direct transfer between the mobile node and the correspondent node is not allowed, and the mobile traffic is in any case to be controlled by the PGW entity.

5.4.1. *Trusted Wi-Fi access*

The establishment of the S2c tunnel constitutes one of the different phases of the mobile attachment described in Figure 5.12.

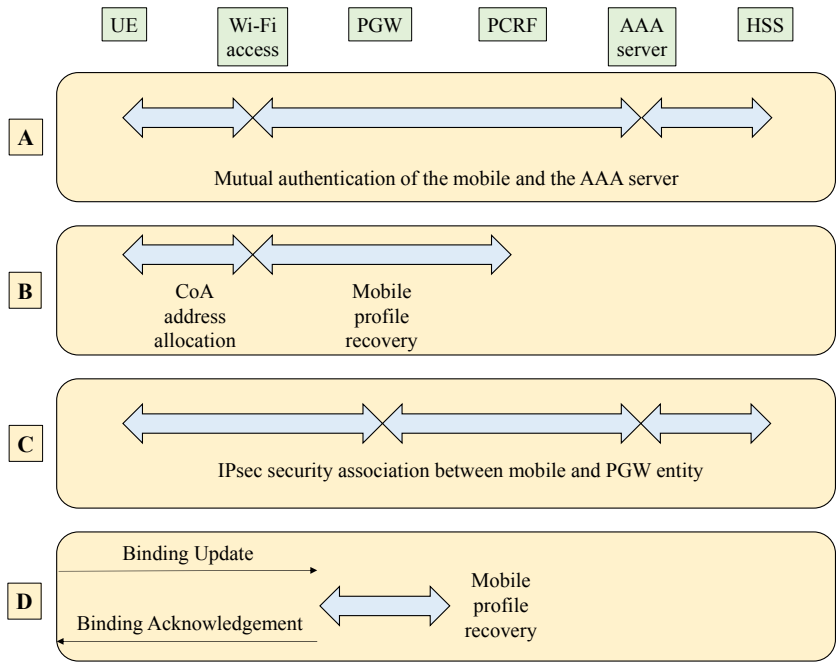

Figure 5.12. *S2c tunnel establishment: trusted Wi-Fi access*

Phase (A) corresponds to the mutual authentication procedure described in section 5.1. At the end of phase (A), the trusted Wi-Fi access has retrieved the service profile of the mobile stored in the HSS entity.

Phase (B) corresponds to the configuration of the mobile via the trusted Wi-Fi. At the end of phase (B), the mobile recovers its CoA. The trusted Wi-Fi access can also initiate a session with the PCRF to retrieve the profile of the mobile stored in the SPR database.

Phase (C) is the establishment of an IPSec association between the mobile and the PGW entity to protect the DSMIPv6 control messages. The principles for establishing a security association are described in section 5.2. At the end of

phase (C), the PGW entity assigns the mobile its HoA and retrieves the service profile of the mobile stored in the HSS entity.

During phase (D), the mobile communicates to the PGW entity the HoA and CoA in the Binding Update message of the Mobility extension of the IPv6 header. In this phase, the PGW entity can also initiate a session with the PCRF entity to retrieve the profile of the mobile stored in the SPR entity. The PGW terminates phase (D) by issuing the Binding Acknowledgment message of the Mobility extension of the IPv6 header. At the end of phase (D), the IP tunnel S2c is established between the mobile and the PGW entity.

5.4.2. *Untrusted Wi-Fi access*

The establishment of the S2c tunnel constitutes one of the different phases of the mobile attachment described in Figure 5.13.

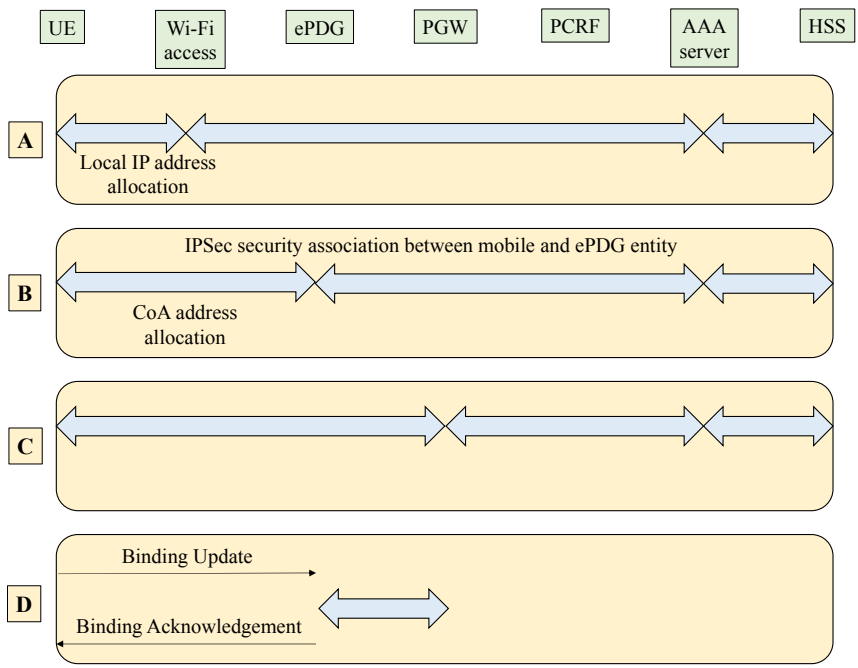

Figure 5.13. *S2c tunnel establishment: untrusted Wi-Fi access*

Phase (A) corresponds to the authentication procedure described in section 5.1. At the end of phase (A), the untrusted Wi-Fi access has retrieved the service profile of the mobile stored in the HSS entity. The untrusted Wi-Fi access provides the mobile with a Local IP Address to start Phase (B) of the procedure.

Phase (B) corresponds to the procedure for establishing the SWu tunnel described in section 5.2. At the end of phase (B), an IPSec tunnel is established between the mobile and the ePDG entity; the ePDG entity has retrieved the service profile of the mobile stored in the HSS entity and assigned the mobile with its CoA.

Phase (C) is the establishment of an IPSec association between the mobile and the PGW entity to protect the DSMIPv6 control messages. At the end of phase (C), the PGW entity allocates the mobile to its HoA and retrieved the mobile service profile stored in the HSS entity.

During phase (D), the mobile communicates to the PGW entity the HoA and CoA in the Binding Update message of the Mobility extension of the IPv6 header. In this phase, the PGW entity can also initiate a session with the PCRF entity to retrieve the profile of the mobile stored in the SPR entity. The PGW entity terminates phase (D) by issuing the Binding Acknowledgment message of the Mobility extension of the IPv6 header. At the end of phase (D), the IP tunnel S2c is established between the mobile and the PGW entity.

6

Wi-Fi Integration – Network Discovery and Selection

6.1. Mechanisms defined by 3GPP organization

6.1.1. *ANDSF function*

The selection of the access network and the management of the traffic between LTE (Long-Term Evolution) access and Wi-Fi (Wireless Fidelity) access are supported by the ANDSF (Access Network Discovery and Selection Function) server.

The configuration data are provided by the ANDSF server and are organized in a hierarchical structure called the device management tree. The exchange of the management object (MO) between the ANDSF server and the mobile is based on extensible markup language (XML).

The mobile can reach the ANDSF server via Wi-Fi access to the Internet or via Wi-Fi access or LTE access to the 4G mobile network.

The ANDSF server can push the information to the mobile (push mode) or the mobile can interrogate the ANDSF server and receive the corresponding information (pull mode). If the mobile submits a request, then it may also include other information in its request, such as its location and the list of discovered radio access networks.

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

The mobile can discover the ANDSF server in one of the following configurations:

– static configuration;

– DNS (Domain Name System) resolution for which a specific full qualified domain name (FQDN) is used

andsf.mnc <MNC> .mcc <MCC> .pub.3gppnetwork.org

– dynamic configuration by a DHCP (Dynamic Host Configuration Protocol) server.

The ANDSF server determines the access on which the mobile must transfer the IP (Internet Protocol) flow in the following cases:

– the mobile is able to route IP packets via a single type of access, LTE or Wi-Fi;

– the mobile is able to route different IP packets for the same PDN (Packet Data Network) connection via different access networks;

– the mobile is able to route IP packets for different PDN connections via different access networks.

The information provided by the ANDSF server may also be preconfigured by the home operator on the terminal or provisioned on the universal integrated circuit card (UICC).

6.1.1.1. *ANDI*

Following a mobile request, the ANDSF server can provide access network discovery information (ANDI) in the vicinity of the mobile (Figure 6.1):

– the types of access technologies, such as the Wi-Fi interface;

– the identifier of the access network, such as the service set identifier (SSID);

– specific information on the characteristics of the radio interface, such as the frequency of the radio channel;

– the conditions indicating when the ANDI is valid.

6.1.1.2. *ISMP*

The inter-system mobility policy (ISMP) provides the mobile with the rules for routing IP packets over LTE or Wi-Fi interfaces. The mobile uses these rules when it cannot access both interfaces simultaneously.

Figure 6.2 describes the structure of the management objects (MO) for the ISMP.

Each ISMP rule includes the following information:

– the validity of the rule. These conditions may include, for example, a duration or a location area;

– a priority list of access technologies to inform the mobile of the order in which they are preferred or restricted access for the connectivity to the evolved packet core (EPC);

– a rule priority to inform the mobile of the level of priority of this rule compared to other ISMP rules provided by the same 4G mobile network.

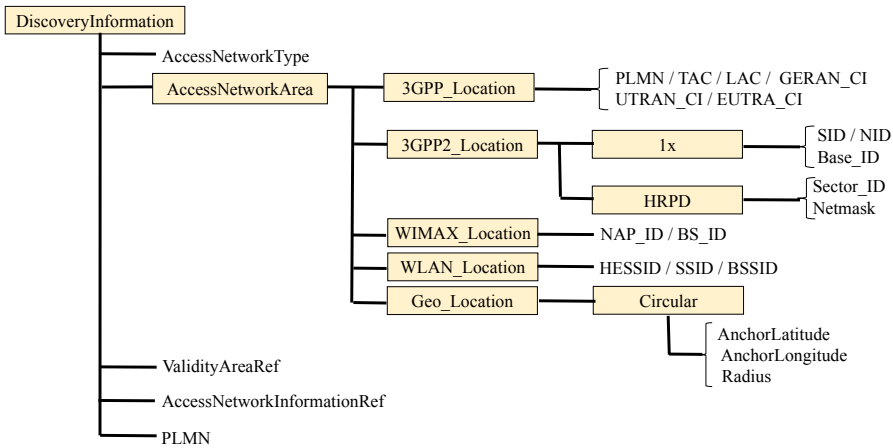

Figure 6.1. *ANDI*

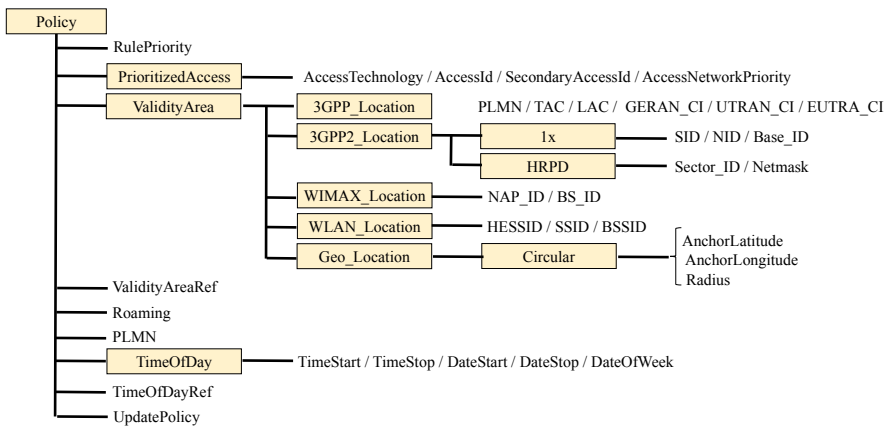

Figure 6.2. *ISMP*

6.1.1.3. *ISRP*

The inter-system routing policy (ISRP) is a set of operator-defined rules that determine how the mobile should route traffic across multiple radio access interfaces.

The IFOM (IP Flow Mobility) rules identify a prioritized list of radio access technologies that should be chosen by the mobile to route the different IP packets of a PDN connection that corresponds to an access point name (APN).

As the PDN connection is anchored in the EPC network, seamless continuity for each IP flow is provided between LTE and Wi-Fi accesses.

Figure 6.3 describes the structure of managed objects (MO) for IFOM rules.

An IFOM rule can also identify which radio accesses are restricted for the traffic, for example, IP packets containing voice must not use Wi-Fi interface.

Each IFOM rule can identify the traffic based on the IP address of the source or destination, the transport protocol, the port numbers of the source or destination, or the DSCP (DiffServ Code Point) or TC (Traffic Class) field.

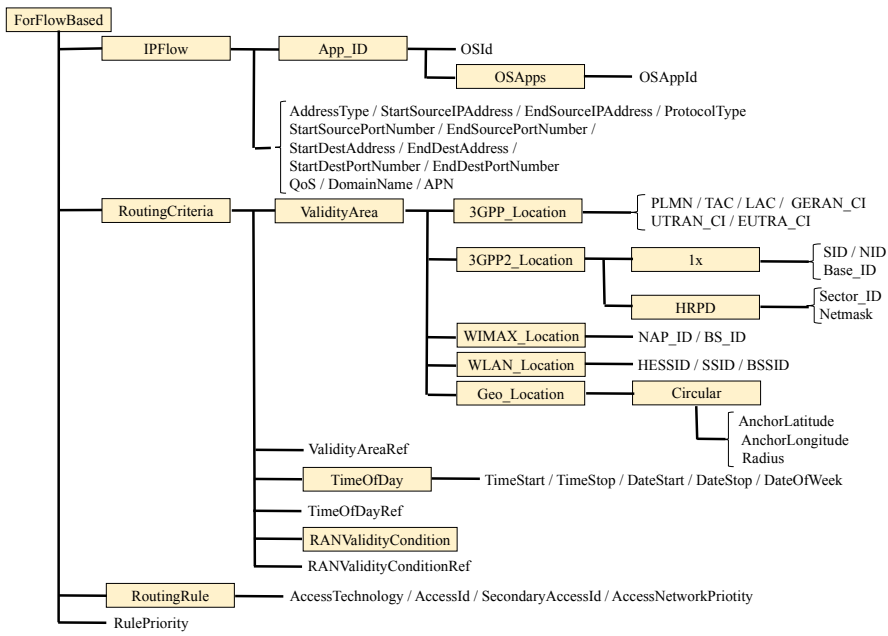

Figure 6.3. *IFOM rules*

The MAPCON (Multi-Access PDN Connectivity) rules identify a prioritized list of radio access technologies that should be used by the mobile to route each PDN connection that corresponds to an access point name (APN).

As the PDN connection is anchored in the EPC network, seamless continuity for each PDN connection is provided between LTE and Wi-Fi accesses.

Figure 6.4 describes the structure of managed objects (MO) for MAPCON rules.

A MAPCON rule can also identify which radio access is restricted for PDN connections; for example, Wi-Fi interface must not be used for certain types of access points (APN).

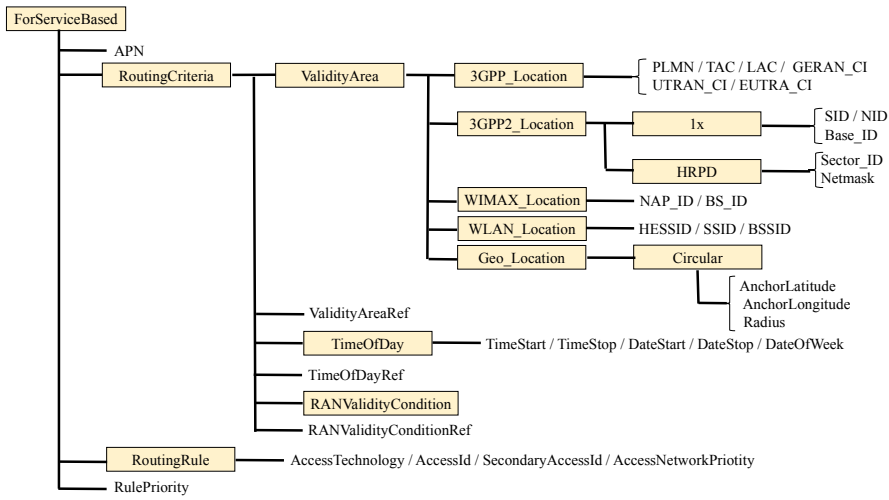

Figure 6.4. *MAPCON rules*

The NSWO (Non-Seamless WLAN Offload) rules identify which IP packets should be offloaded by Wi-Fi access to the Internet network without crossing the EPC network.

Because streams are not anchored in the EPC network, seamless continuity for each IP stream is not assured between LTE and Wi-Fi accesses.

It is possible to restrict or allow the offloading of traffic to specific Wi-Fi access networks.

Figure 6.5 describes the structure of managed objects (MO) for NSWO rules.

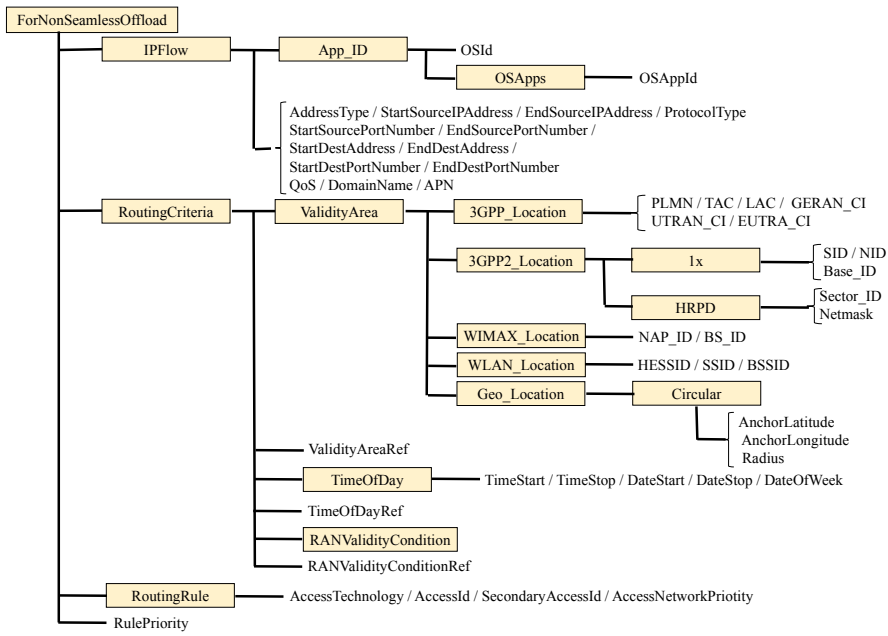

Figure 6.5. *NSWO rules*

6.1.1.4. *IARP*

The IARP (Inter-APN Routing Policy) rules determine which traffic should be routed across different PDN connections and which traffic should be offloaded by Wi-Fi access to the Internet network (Figure 6.6).

The rules for the access point (APN) identify a prioritized list of access point names that should be used by the mobile to route traffic that matches IP traffic filters.

The rules for NSWO identify which traffic should be offloaded for Wi-Fi access to the Internet network.

When the mobile has both the IARP rule and the ISRP rule simultaneously, it first evaluates the IARP rules to determine how to route an IP stream. If the IP stream does not match any IARP rules, the mobile evaluates the active ISRP rules to determine how to route the IP stream.

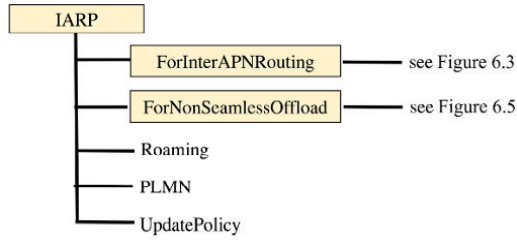

Figure 6.6. *IARP rules*

6.1.1.5. *WLANSP*

The WLANSP is a set of rules that determine how the mobile selects a Wi-Fi access network.

Figure 6.7 describes the structure of the managed objects (MO) for the WLANSP.

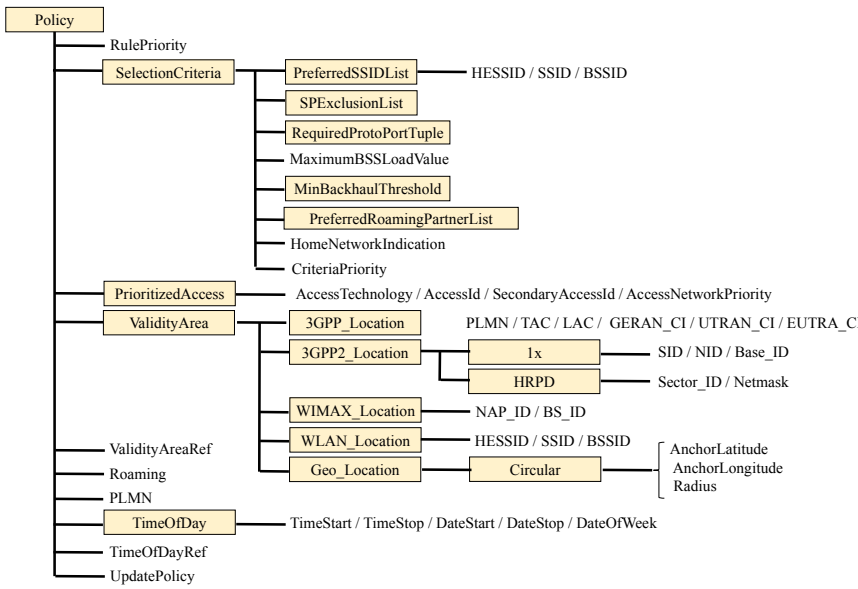

Figure 6.7. *WLANSP*

Each WLANSP rule includes the following information:

– the conditions indicating when the rule is valid. The conditions of validity can include the time, geolocation and location of the network, such as the location area;

– the selection criteria that must be fulfilled by the Wi-Fi access network to be eligible, such as cell load or transmission network throughput.

6.1.1.6. *Wi-Fi access network preferences*

Network preferences include information that helps the mobile to select a Wi-Fi access network.

The network preferences indicate whether the network prefers the mobile to establish a PDN connection using the S2a architecture or not.

In the case of a PDN connection using the S2b architecture, the network preferences indicate the identity of the evolved packet data gateway (ePDG).

The EHSP (Equivalent Home Service Providers) information contains a list of service providers that are equivalent to the mobile home network. Each service provider is identified with a domain name.

The PSPL (Preferred Service Provider List) information contains a preferred list of service providers.

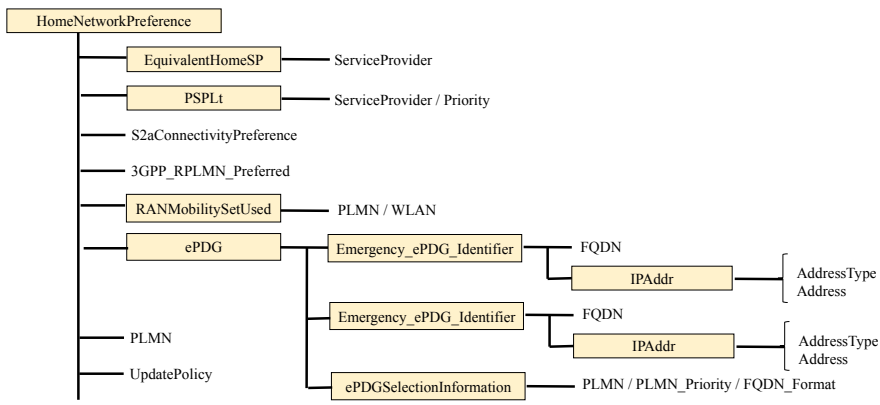

Figure 6.8. *Wi-Fi access network preferences*

6.1.2. *RAN assistance*

The evolved node base station (eNB) can provide mobile support information. This information includes the following parameters:

– the thresholds for access to the LTE interface;

– the thresholds for the Wi-Fi interface;

– the offload preference indication (OPI).

The thresholds for the LTE interface define the high and low values of the radio parameters, for example the average value of the reference signal received power (RSRP).

The thresholds for the Wi-Fi interface define the high and low values of the access parameters, such as the received signal strength indication (RSSI) of the beacon, the transmission network throughput and the load of the radio channel.

The OPI is a one-dimensional bitmap that can be used by mobiles to determine when they should move certain traffic to Wi-Fi access or LTE access. The meaning of each bit is operator specific.

The thresholds and parameters can affect the validity of ANDSF rules and thus make these rules subject to the conditions defined by the eNB entity.

The thresholds and parameters can be used by the following ANDSF rules:

– the ISRP rules, including IFOM rules, MAPCON rules and NSWO rules;

– the IARP rules, including rules related to the access point name (APN) and NSWO.

The selection of the Wi-Fi interface and the routing behavior for the mobile must be controlled either by the ANDSF rules or by the rules provided by the eNB entity, and not by a combination thereof.

The only exception is the simultaneous enforcement of the rules provided by the eNB entity and the IARP rules for the APN.

6.2. Mechanisms defined by IEEE and WFA organizations

Before associating with an access point, the mobile requires information on the services provided by the Wi-Fi access networks, from GAS (Generic Advertisement Service) frames that are Action-type management frames.

The Public Action field, in the byte immediately after the Category field, differentiates the types of Action frames.

GAS frames provide transparent transport of a list with ANQP (Access Network Query Protocol) elements to communicate information.

The Interworking element in the management frames Beacon or Probe Response indicates that the GAS protocol is supported (Figure 6.9).

The Advertisement Protocol element in the management frames Beacon or Probe Response indicates that the ANQP protocol is supported (Figure 6.9).

The mobile transmits a request in a GAS Initial Request frame and the access point provides the requested information or information on how to receive the response in the GAS Initial Response frame (Figure 6.9).

The response to the GAS Initial Request frame is provided in this case in one or more GAS Comeback Response frames.

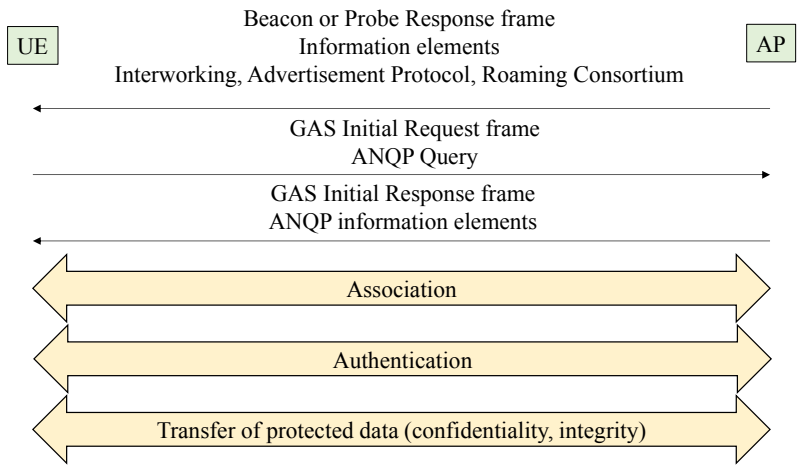

Figure 6.9. *GAS/ANQP exchanges*

The response to the GAS Initial Request frame shall not be shared between an Initial Response GAS frame and one or more Comeback Response GAS frames.

The access point has the information elements or transfers the request from the mobile to an ANQP server.

The IEEE (Institute of Electrical and Electronics Engineers) has defined a subset of ANQP information elements (Table 6.1).

The WFA (Wi-Fi Alliance) has completed this list as part of the Passpoint certification based on Hotspot 2.0 features (Table 6.1).

ANQP information elements	Specification	Function
3GPP Cellular Network	IEEE	Identification and authentication methods from the service provider
NAI Realm	IEEE	
Roaming Consortium	IEEE	
Domain Name	IEEE	Identification of the Wi-Fi access network
Venue Name	IEEE	
Operator's Friendly Name	WFA	
IP Address Type Availability	IEEE	
WAN Metrics	WFA	Characteristics of the Wi-Fi access network
Connection Capability	WFA	
Operating Class Indication	WFA	
Network Authentication Type	IEEE	
OSU Providers List	WFA	Online registration
Icon Request & Response	WFA	
HS Query List	WFA	Capacity request
HS Capability List	WFA	
NAI Home Realm Query	WFA	

Table 6.1. *ANQP information elements*

6.2.1. *Information elements provided by the beacon*

6.2.1.1. *HESSID element*

If two access points have different SSID, they are considered as different Wi-Fi networks. If two access points have the same SSID, they are considered as part of the same wireless network.

However, since SSID are not globally administered, it is possible that two access points with the same SSID concern different Wi-Fi networks.

The homogeneous extended service set identifier (HESSID) allows mobiles to detect this condition. When two access points of two different Wi-Fi networks have the same SSID, the two networks are differentiated by two different HESSID.

The HESSID is included in the Interworking element in Beacon or Probe Response frames.

The HESSID is a MAC (Medium Access Control) address. The HESSID value has the same value as the basic service set identifier (BSSID) of one of the access points.

6.2.1.2. *Access Network Type field*

The Access Network Type field is included in the Interworking element. Mobiles can use this information when selecting an access point.

The Access Network Type field indicates the type of network to which the access point is connected: pay public network, free public network, private network and private network with guest access.

6.2.1.3. *Internet Available field*

The Internet Available field is included in the Interworking element. This field informs mobiles as to whether access to the Internet is available at the access point, which may not be the case in environments where the operator (e.g. a museum) may limit Wi-Fi access to only local content.

6.2.1.4. *BSS Load element*

The BSS Load information element contains information on the use of the radio channels and the number of associated mobiles on the access point. The mobile uses this information when selecting a network.

6.2.2. *Information elements provided by the ANQP server*

6.2.2.1. *3GPP Cellular Network element*

The information element 3GPP Cellular Network contains the identity of the 4G mobile network. It allows the mobile to check from its universal subscriber

identity module (USIM) if the Wi-Fi network operator has a roaming agreement with the 4G mobile network operator.

The identity of the 4G mobile network consists of the mobile country code (MCC) and the mobile network code (MNC) allocated to the operator.

If the information element 3GPP Cellular Network matches any identity stored in the mobile, then it prioritizes this access point for the association.

6.2.2.2. *NAI Realm element*

The information element NAI Realm provides a list of domains identified by the network access identifier (NAI) for service providers that can authenticate a mobile with either a user ID or a password or a certificate.

Each entry in the NAI Realm list can identify the EAP (Extensible Authentication Protocol) methods that are supported for authentication.

6.2.2.3. *Roaming Consortium element*

The information element Roaming Consortium provides a list of roaming consortium identifiers and service provider partners with roaming agreements.

The information element Roaming Consortium is broadcasted in the management frame Beacon or transmitted in the Probe Response frame. A mobile may request an information element Roaming Consortium if the information received is insufficient for the selection of the network.

6.2.2.4. *Domain Name element*

The information element Domain Name provides a list of one or more domain names of the entity that operates the Wi-Fi network.

The mobile uses the domain name to determine whether access to this Wi-Fi network through this access point is considered access to its home network or to a visited network.

6.2.2.5. *Venue Name element*

The information element Venue Name provides venue names that can be used to help the mobile to select the access point. The names of the venue can be included in the same language or in different languages.

6.2.2.6. *Operator's Friendly Name element*

The information element Operator's Friendly Name provides the friendly name of the Wi-Fi network operator.

The mobile can obtain the name of the operator via GAS/ANQP requests to help the user when manually selecting access points.

6.2.2.7. *IP Address Type Availability element*

The information element IP Address Type Availability provides information about IP addresses and port numbers:

– Wi-Fi access point allocates a public IPv4 address;

– Wi-Fi access point allocates a private IPv4 address;

– the combination of the Wi-Fi access network and the core network allocates a dual NAT IPv4 address;

– Wi-Fi access point allocates an IPv6 address.

6.2.2.8. *WAN Metrics element*

The information element WAN Metrics provides information about the link that connects the access point to the Internet network: the state of the link, and the value of the bit rates for each direction of transmission.

The access point may also provide additional information, such as the load for each direction of transmission.

The mobile uses this information to make network selection decisions. The mobile determines whether the available rate level is compatible with the application need.

6.2.2.9. *Connection Capability element*

The information element Connection Capability provides information about the allowed values of the Protocol field of the IPv4 header or Next Header field of the IPv6 header and port numbers.

The mobile uses this information to make network selection decisions. The mobile determines whether the allowed values are compatible with the characteristics of the application.

6.2.2.10. *Operating Class Indication element*

The information element Operating Class Indication provides information about the radio channels and frequency bands used by the access point.

The mobile uses this information to make network selection decisions. If the mobile supports the 2.4 and 5 GHz frequency bands, and if these two frequency bands are available at the access point, then the mobile will select the 5 GHz band.

6.2.2.11. *Network Authentication Type element*

The information element Network Authentication Type provides a list of authentication types:

– the network requires the user to accept the terms and conditions;

– the network supports online registration;

– the network infrastructure performs HTTP/HTTPS redirection;

– the network supports a DNS redirection.

6.2.2.12. *OSU Providers List element*

The information element OSU Providers List contains a list of entities that offer an online registration service.

The information element OSU Providers List provides a list of available icons that can be displayed by the mobile. This list contains the definition of the image, the image type, the language and the name of the file. This information allows the mobile to determine the icon to download and the file name of the icon to recover.

6.2.2.13. *Icon Request & Response element*

The information element Icon Request & Response allows the mobile to send a request containing the file name of the icon and to return to the access point the answer containing the download status code, the length of the type of icon, the data length and binary icon data.

6.2.2.14. *HS Query List element*

The information element HS Query List is transmitted by the mobile to obtain information simultaneously on several elements of ANQP information.

The information element HS Query List is transmitted in a GAS Query Request frame.

6.2.2.15. *HS Capability List element*

The information element HS Capability List informs the mobile of which ANQP elements are supported by the access point.

The information element HS Capability List is transmitted in a GAS Query Response frame.

6.2.2.16. *NAI Home Realm Query element*

The information element NAI Home Realm Query enables the mobile to determine whether the domains for which it has security information correspond to the service providers whose networks are accessible at the access point.

7

LLC Service – Proximity Communications

7.1. Introduction

The proximity service (ProSe) enables a new type of link, the sidelink (SL), between mobiles, in addition to the downlink (DL) and uplink (UL) between a mobile and an evolved node base station (eNB).

The proximity service implements two types of communication:

– device-to-device (D2D) communication;

– vehicle-to-everything (V2X) communication.

The D2D communication comes in two applications:

– communication between mobiles related to public safety (e.g. firefighters);

– communication between mobiles for commercial purposes.

The mobile communication between mobiles related to public security allows the service to be maintained when the eNB entity fails, for example, in a large-scale disaster or when mobiles are no longer covered by the eNB entity.

The distribution of information to nearby terminals is a function introduced for mobile communication for commercial purposes.

In the coverage scenario, the radio access network controls the resources used for the D2D communication. It can assign to a mobile-specific resource or a pool of resources from which the mobile selects. In this way, interference with cellular traffic is avoided.

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

In the case of the mobile being out of coverage, control over the radio access network is not possible. The mobile uses preconfigured resources, either on the equipment or in the universal subscriber identity module (USIM) of the universal integrated circuit card (UICC).

A special case is partial coverage. The out-of-coverage mobile uses preconfigured values, while in coverage case, the mobile obtains its resources from the eNB entity. The coordination between the radio access network and the preconfigured values is necessary to allow communication and to limit interference to mobiles at the edge of the cell.

Figure 7.1 summarizes the various scenarios for deploying D2D communications:

– both mobiles (UE A and UE B) are not covered by the eNB entity;

– a single mobile (UE A) is under the coverage of the eNB entity;

– the two mobiles (UE A and UE B) are under the coverage of a single eNB entity;

– the two mobiles (UE A and UE B) are under the coverage of two eNB entities (eNB A and eNB B).

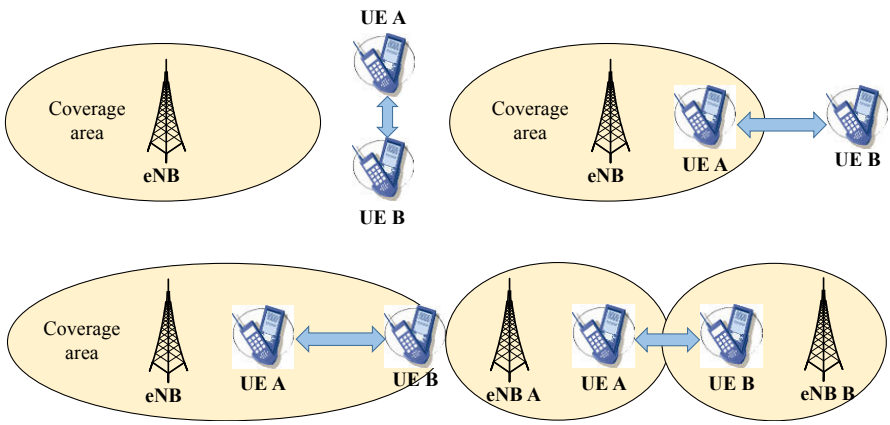

Figure 7.1. *Deployment scenarios for D2D communications*

The four types of deployment are applicable to the mobile communication related to public safety. Deployment is restricted for mobile-to-commercial communications, with mobiles being under eNB coverage.

The V2X communication is divided into four types of communication depending on the different devices with which the vehicle connects (Figure 7.2):

– vehicle-to-vehicle (V2V) communication;

– vehicle-to-infrastructure (V2I) communication;

– vehicle-to-pedestrian (V2P) communication;

– vehicle-to-network (V2N) communication.

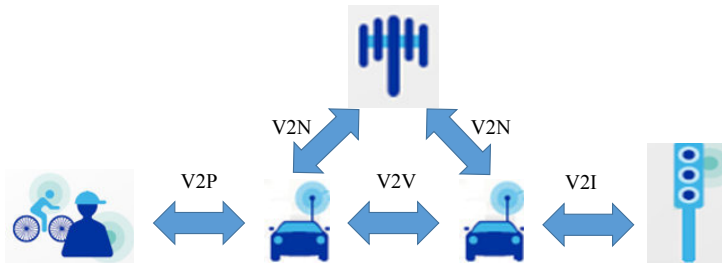

Figure 7.2. *Different types of V2X communication*

V2V and V2P communications use the sidelink communication defined for the D2D communication with the following enhancements:

– taking into account the Doppler effect linked to high relative speeds up to 500 km/h and the synchronization outside the coverage of the eNB entity;

– taking into account the densification with better allocation of resources and congestion control.

V2N communications use the radio interface LTE-Uu.

V2I communications use either the radio interface LTE-Uu or the sidelink communication.

7.2. Functional architecture

7.2.1. *D2D communication*

The functional architecture (Figure 7.3) introduces, as the central entity for D2D communications, the ProSe function that communicates with the following elements:

– the user equipment (UE) for authorization and configuration;

– the home subscriber server (HSS) to retrieve authentication and subscription data from the service;

– the SUPL (Secure User Plane Location) location platform (SLP) to retrieve the location data of the mobile;

– the ProSe application server (AS) to register applications.

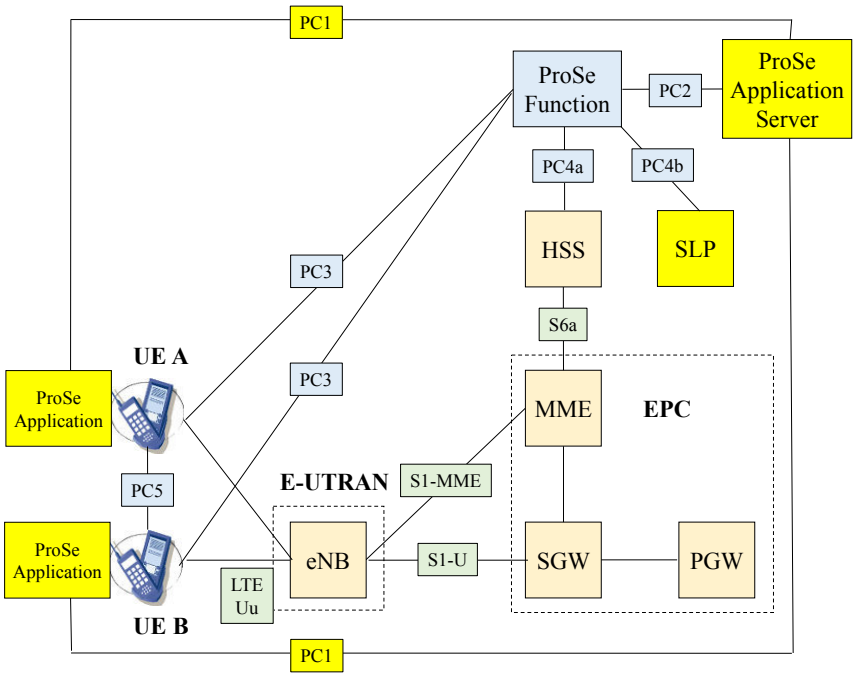

Figure 7.3. *Functional architecture: D2D communications*

7.2.1.1. *ProSe function*

The ProSe function includes direct provisioning, direct discovery name management and EPC-level discovery sub-features.

The direct provisioning sub-function is used to configure the mobile with the necessary parameters for using direct discovery and sidelink communication functions.

The direct discovery name management sub-function is used for the unrestricted direct discovery function to process the mapping of ProSe application credentials and ProSe application codes.

If the mobile is authorized to transmit the ProSe application identifier in the Discovery Request message, the network will allocate the corresponding ProSe application code via a Discovery Response message including a validity timer.

The ProSe application identifier has two parts:

– the operator identifier, consisting of the mobile country code (MCC) and the mobile network code (MNC);

– the application identifier, consisting of several tags separated by a dot, the first tag being always named ProSe App.

The ProSe application code consists of two parts:

– the identifier of the operator, completed by the Scope field and the E bit;

– a temporary identifier to replace the identifier of the application.

The Scope field indicates whether the operator identifier has a global scope, whether it is country-specific or operator-specific identifier.

The E bit determines whether or not the identifier of the operator who assigned this particular code is included in the ProSe application code.

The direct discovery name management sub-function uses ProSe service-related subscriber data stored in the HSS entity to obtain authorization for each discovery request.

The direct discovery name management sub-function also provides the mobile with the necessary security materials to protect discovery messages.

The direct discovery name management sub-function is used for the restricted direct discovery to obtain authorization for discovery requests from the ProSe application server.

The EPC-level discovery sub-function has a reference point to the ProSe application server (PC2), other ProSe functions (PC6 or PC7), the HSS entity (PC4a), the SLP entity (PC4b) and the mobile (PC3).

The EPC-level Discovery sub-function provides the following:

– the storage of subscriber data related to the ProSe service and/or the retrieval of subscriber data from the HSS entity;

– the authorization and the configuration of the mobile for direct discovery and sidelink communication;

– the storage of a list of applications allowed to be used for direct discovery and sidelink communication;

– the agent to the SLP location entity to enable the direct discovery;

– the exchange of signaling with application servers for the registration of applications;

– the exchange of signaling with ProSe functions located in other networks for sending proximity requests, proximity alerts and location reports;

– the optional support for the mobile location request via the HSS entity.

7.2.1.2. *Protocol architecture*

The PC1 interface is the reference point between the ProSe application hosted on the mobile and the ProSe application server. This interface is not defined as part of the mobile network architecture.

The PC2 interface is the reference point between the ProSe application server and the ProSe function. This interface supports the DIAMETER protocol for recording ProSe applications.

The PC3 interface is the reference point between the mobile and the ProSe function. This interface supports the hypertext transfer protocol (HTTP) that transports data in XML (eXtensible Markup Language) format for mobile authorization and configuration.

The IP (Internet Protocol) packet containing the HTTP/XML message is transported in the following bearers (Figure 7.4):

– the radio bearer built on the LTE-Uu interface between the mobile and the eNB entity;

– the S1-U bearer built between the eNB and SGW (Serving Gateway) entities;

– the S5 bearer built between SGW and PGW (PDN [Packet Data Network] Gateway) entities.

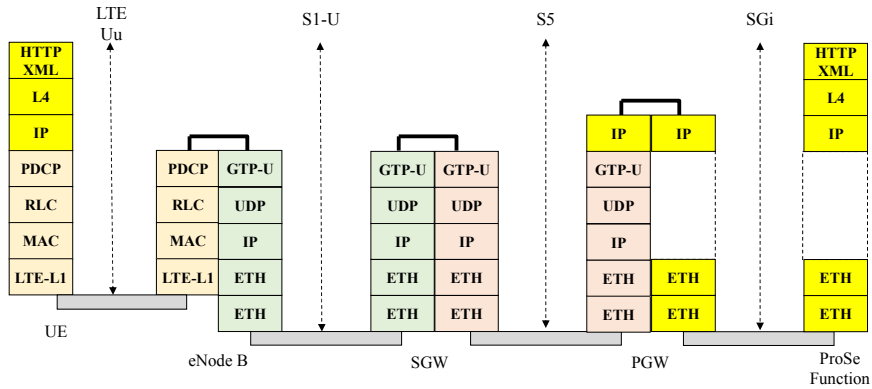

Figure 7.4. *Transport of the HTTP/XML message*

The PC4a interface is the reference point between the ProSe function and the HSS entity. This interface supports the DIAMETER signaling for the transfer of authentication and subscription data to the service.

The PC4b interface is the reference point between the ProSe function and the SLP entity. This interface supports the mobile location protocol (MLP) for mobile location.

The PC5 interface is the reference point between mobiles A and B. This interface supports the discovery protocol, the signaling and the traffic data. The transmission on the PC5 interface can be in the unicast or broadcast mode.

The PC6 interface is the reference point between the ProSe functions of networks A and B. This interface is used when mobiles A and B are respectively connected to networks A and B.

The PC7 interface is the reference point between the ProSe function of the home and the visited network. This interface is used in the case of roaming.

The PC6 and PC7 interfaces support the DIAMETER protocol for the transfer of mobile location data.

7.2.2. *V2X communication*

The functional architecture (Figure 7.5) introduces, as the central entity for V2X communications, the V2X control function which informs the mobile with the

parameters necessary to use the V2X communication and which communicates with the HSS entity and the V2X application servers.

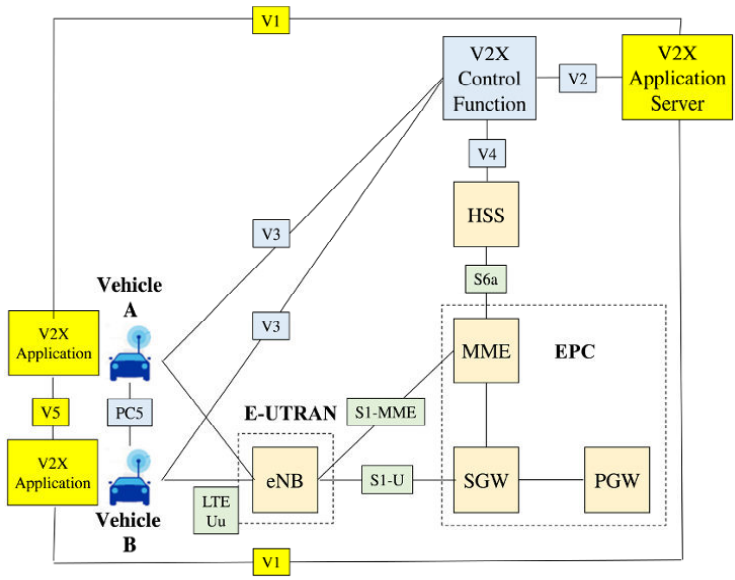

Figure 7.5. *Functional architecture: V2X communications*

The road side unit (RSU) is a fixed infrastructure entity capable of receiving and sending V2X messages. Two types of RSUs are defined (Figure 7.6):

– the eNB-type RSU: the fixed infrastructure, ensuring the transmission of V2X messages to mobiles via the LTE-Uu reference point, is associated with the eNB entity;

– the UE-type RSU: the fixed infrastructure, ensuring the transmission of V2X messages to mobiles via the PC5 reference point, is associated with a fixed UE, itself connected via the LTE-Uu reference point to an eNB entity.

The V1 interface is the reference point between the V2X application server hosted in the mobile (vehicle, pedestrians and infrastructure) and the V2X application server. This interface is not defined as part of the mobile network architecture.

The V2 interface is the reference point between the V2X application server and the V2X control function. The V2X application server uses this interface to provide its information to the network.

The V3 interface is the reference point between the mobile and the V2X control function. The V2X control function in the home network is the entity that grants the mobile with the authorization to use the V2X communication service.

The V4 interface is the reference point between the V2X control function and the HSS entity. The V2X control function uses the HSS entity to obtain general information about the mobile subscription.

The V5 interface is the reference point between the V2X applications of mobiles A and B. This interface is not defined as part of the mobile network architecture.

The V6 interface is the reference point between the V2X control function of the home and the visited network. This interface is used in the case of roaming.

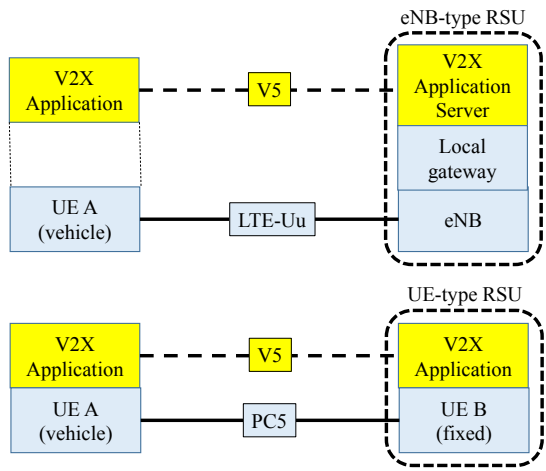

Figure 7.6. *eNB-type and UE-type RSU*

7.3. Direct discovery

The network is informed during the attachment procedure if the mobile supports proximity services. Direct discovery and direct communication are autonomous services:

– direct discovery is not necessarily followed by direct communication;

– direct communication does not require direct discovery as a precondition.

The discovery is divided into open discovery and restricted discovery. In the latter case, an explicit authorization is required for the mobile being discovered.

The direct discovery is commercially enabled only for the radio coverage scenario and is therefore entirely under the control of the network.

Two modes are defined for using the discovery:

– the mobile broadcasts information about itself;

– the mobile sends a request containing certain information on what interests it.

For a mobile intended to be used for public safety, the required service authorization may be stored in the device itself or in the USIM of the UICC.

After authorization, the next step is to send a Discovery Request message to the network. This request is processed by the ProSe function.

The ProSe function contacts the HSS entity to verify that the application is allowed for direct discovery. The ProSe function checks whether the mobile is allowed to use the ProSe application code for announcing or monitoring and prepares a Discovery Response message for the mobile.

For the announcement, the ProSe function returns the ProSe application code and a validity timer. When the timer expires, the mobile must request a new code from the network.

For the monitoring, the Discovery Response message contains one (or more) discovery filter and associated filter identifiers.

If the mobile configured for the monitoring receives a ProSe application code that matches the assigned discovery filter, but does not have a corresponding ProSe application identifier, it is required to send a matching report to the ProSe function.

In this correspondence report, the mobile must indicate whether it wishes to receive data regarding the associated ProSe application identifier. The ProSe function uses the information provided for validation and verification. If this operation succeeds, it sends an acknowledgment to the mobile.

7.4. Radio interface

7.4.1. *Radio interface structure*

The PC5 radio interface introduces new types of channels and signals (Figure 7.7):

– the logical channels which constitute the interface between the RLC (Radio Link Control) and MAC (Medium Access Control) layers;

– the transport channels which constitute the interface between the MAC layer and the physical layer;

– the physical channels which constitute the internal interface to the physical layer, between, on the one hand, the coding functions of the channel, and, on the other hand, the modulation and multiplexing functions;

– the physical synchronization signals.

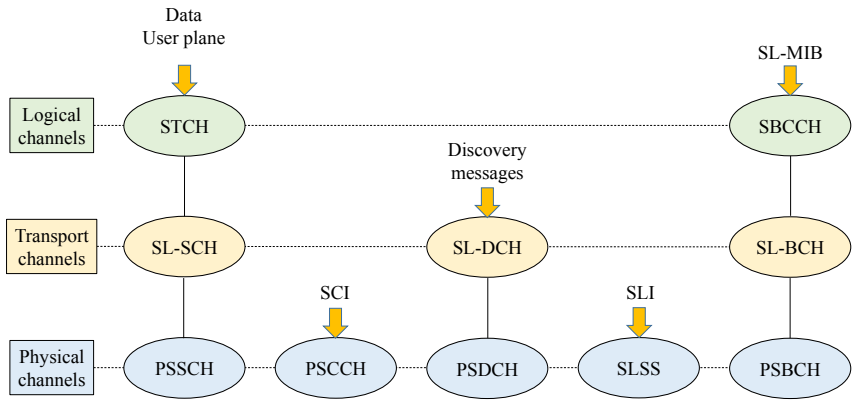

Figure 7.7. *Radio interface structure*

The sidelink traffic channel (STCH) is used for exchanging user plane data and is mapped to the sidelink shared channel (SL-SCH). The SL-SCH transport channel is then mapped to the Physical Sidelink Shared Channel (PSSCH).

In order for the mobile reception chain to process the PSSCH, the sidelink control information (SCI) is mapped to the physical sidelink control channel (PSCCH).

The radio resources for the sidelink communication can be selected autonomously by the mobile or configured by the network.

The mobile can know the resource blocks allocated to the sidelink communication via the system information block 18 (SIB18) broadcasted by the network.

If this information is not available, the mobile must connect to the network to receive the downlink control information 5 (DCI-5) in the physical downlink control channel (PDCCH) containing the characteristics of the resource blocks allocated to the sidelink communication.

The sidelink discovery channel (SL-DCH) is used by the direct discovery procedure and is mapped to the physical sidelink discovery channel (PSDCH). The discovery function is not used for V2X communications.

The SIB19 provides information on the radio resource pool, on which the mobile is authorized to broadcast (announcing) or receive (monitoring) discovery messages.

The sidelink synchronization signal (SLSS) comprises the primary sidelink synchronization signal (PSSS) and the secondary sidelink synchronization signal (SSSS).

In the case of the D2D communication, the SLSS defines a sidelink identifier (SLI) indicating whether the SLSS is synchronized by the network (value between 0 and 167) or not (value between 168 and 335).

In the case of the V2X communication, the values 0, 168 and 169 of the SLI indicate that the mobile obtains its synchronization from a global navigation satellite system (GNSS).

The sidelink broadcast control channel (SBCCH) contains the sidelink master information block (SL-MIB) containing the technical characteristics of the radio channel assigned to the sidelink.

The SBCCH is mapped to the sidelink broadcast channel (SL-BCH). The SL-BCH is then mapped to the physical sidelink broadcast channel (PSBCH).

The demodulation reference signal (DMRS) is associated with the PSSCH, PSCCH, PSDCH and PSBCH. It is transmitted as the reference signal associated with the physical uplink shared channel (PUSCH) of cellular traffic.

Data transmission over sidelink channels has the same characteristics as the PUSCH of cellular traffic.

The transmission uses single-carrier frequency-division multiple access (SC-FDMA) and applies a quadrature phase-shift keying (QPSK) or a quadrature amplitude modulation (16-QAM) with 16 states.

The QPSK is applied to transmit the control information data on the PSCCH, PSBCH and PSDCH. On the other hand, the user data transmitted on the PSSCH exploits the QPSK and 16-QAM.

7.4.2. *Physical resources*

7.4.2.1. *D2D communication*

A resource pool (RP) is a set of resources assigned to the sidelink. It consists of sub-frames and, within the sub-frames, physical resource blocks (PRBs) (Figure 7.8).

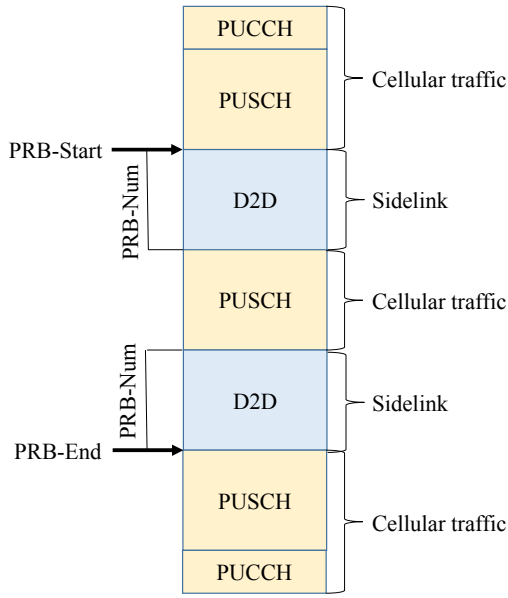

Figure 7.8. *Resources allocated to the sidelink*

There are two resource allocation modes:

– in mode 1 (D2D communication) or mode 3 (V2X communication), the eNB entity indicates the resources to be used for the sidelink;

– in mode 2 (D2D communication) or mode 4 (V2X communication), the mobile selects the resources from a set of allocated pools.

For modes 1 and 3, the mobile must be in the RRC_CONNECTED state, while for modes 2 and 4, the mobile may be in the RRC_IDLE state or even outside the radio coverage of the eNB entity.

In a sub-frame, the resources used are in two bands, identified by the physical resource blocks occupied by the sidelink. The first band starts at PRB-Start and the second band ends at PRB-End, each having a resource block width PRB-Num. This arrangement makes it possible to nest several resource pools in a sub-frame and to use the remaining resource blocks for cellular traffic.

Sub-frames allocated to cellular and sidelink communications are indicated in a sub-frame bitmap, whose sidelink control (SC) periodicity is configurable from 40 ms to 320 ms.

The PSSS and SSSS occupy 62 resource elements in the frequency domain and two adjacent OFDM symbols in the time domain. The PSSS and SSSS are identical to the primary synchronization signal (PSS) and the secondary synchronization signal (SSS) of the cellular traffic and are transmitted in a frame every 40 ms.

For a normal cyclic prefix, the PSSS is transmitted in the OFDM symbols 1 and 2 of the first slot and the SSSS in the OFDM symbols 4 and 5 of the second time slot of the same sub-frame (Figure 7.9).

The PSBCH is transmitted in the same sub-frame as the PSSS and SSSS (Figure 7.9). The PSBCH occupies 72 resource elements (six PRBs) in the frequency domain and the remaining OFDM symbols in the time domain, except for those assigned to the DMRS or the guard time.

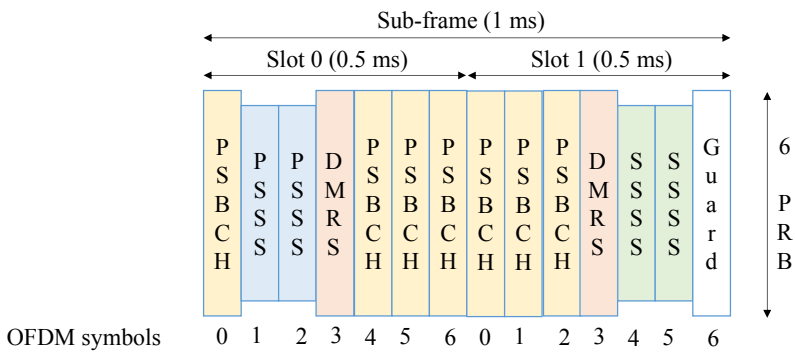

Figure 7.9. *Resources allocated to SLSS and PSBCH*

For mode 1, sub-frames assigned to the PSCCH are indicated in a SubframeBitmapSL bitmap transmitted in the SCI. The region assigned to the traffic starts after the last bit ONE of the bitmap. It consists of a time repetition pattern (TRP) of bitmaps, which indicates the sub-frames assigned to the PSSCH. This bitmap is repeated until the end of the SC period, where the last occurrence can be truncated.

For mode 2, this structure is quite similar. The main difference is that the start of the traffic portion does not depend on the content of the SubframeBitmapSL bitmap, but has a fixed offset from the beginning of the SC period.

The resources allocated to the PSDCH for discovery are similar to those assigned to the PSCCH and PSSCH.

7.4.2.2. *V2X communication*

As with the D2D communication, the vehicle, which uses PC5 sidelink communications, allocates specific time and frequency resources in the form of PRBs for transporting control and user data.

As for the D2D communication, PC5 sidelink communications are allowed in PRBs configured via control messages provided by the eNB entity or preconfigured in the mobile. All sub-frames providing PRBs for PC5 sidelink communications constitute the sub-frame pool.

PRBs are allocated to the sidelink communication in adjacent or non-adjacent manner.

The control plane or user plane data are transmitted in a sub-channel (SCH). The sub-channel division is defined by the network.

In the case of using adjacent PRBs (Figure 7.10):

– the parameter StartRBSubChannel defines the first resource block PRBs of the SCH;

– the parameter SizeSubChannel defines the number of blocks of PRBs resources in an SCH;

– the parameter Number of SubChannels defines the number of SCH established in the sub-frame.

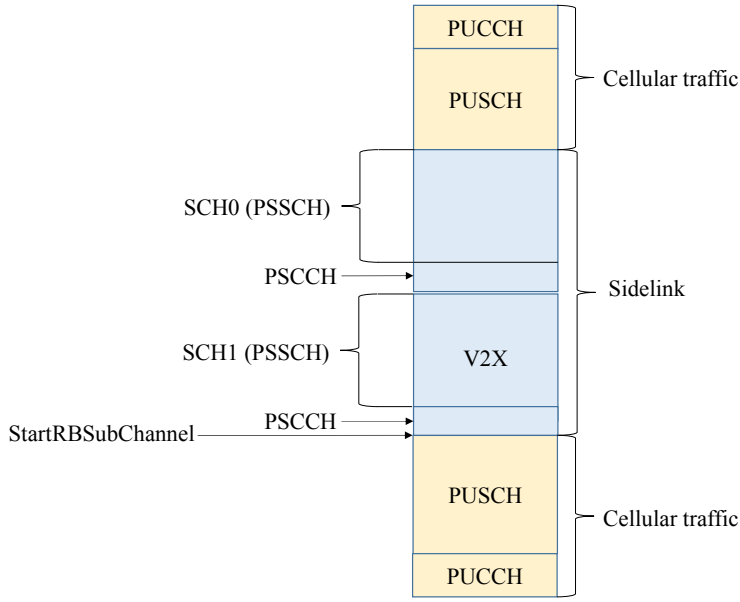

Figure 7.10. *Resources allocated to the sidelink: adjacent resource blocks*

In the case of non-adjacent PRBs (Figure 7.11):

– the parameter StartRBPSCCHPool defines the first PRB allocated to the PSCCH;

– the parameter StartRBSubChannel defines the first PRB of the sub-channel assigned to the PSSCH.

The PRB assigned to the PSCCH for transmitting an SCI message occupy four blocks of contiguous PRBs.

The SLSS and the PBSCH are transmitted with a periodicity of 160 ms.

When the transmission is for the PSCCH and PSSCH, two additional DMRS are inserted into the sub-frames to compensate for interference caused by Doppler shifts (Figure 7.12).

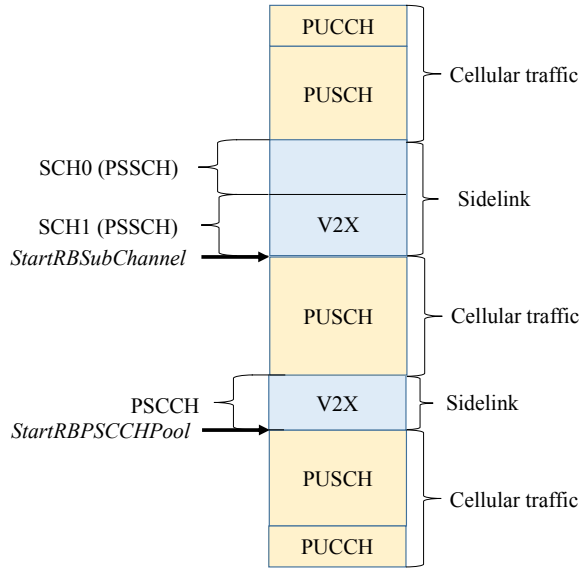

Figure 7.11. *Resources allocated to the sidelink: non-adjacent resource blocks*

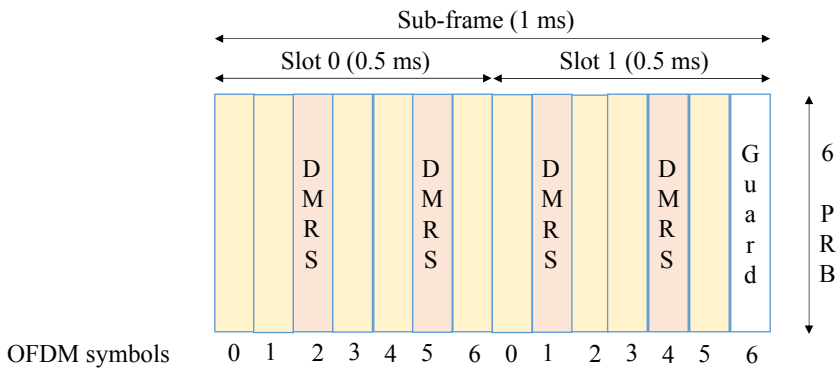

Figure 7.12. *DMRS associated with PSCCH and PSSCH*

When the transmission concerns the SLSS and the PSBCH, three DMRS are conveyed in the symbols 4 and 6 of the first slot and in the symbol 2 of the second slot of the sub-frame (Figure 7.13).

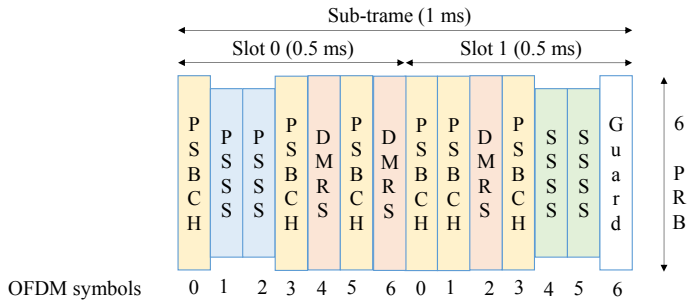

Figure 7.13. *DMRS associated with SLSS and PSBCH*

8

LLC Service – Group Communications

8.1. Introduction

The group communication service (GCS) provides a fast and efficient mechanism for distributing the same content to multiple users in a controlled manner.

The eMBMS (evolved Multimedia Broadcast/Multicast Service) network completes the 4G mobile network architecture by introducing:

– a transport architecture allowing the transmission, for the downstream direction, of IP packets in a multicast bearer;

– a service architecture comprising two domains:

- the security domain ensuring the mutual authentication and the key establishment;

- the application domain ensuring the description and the structuring of the data.

Two functions determine the transmission mode on the radio interface:

– the MBSFN (MBMS over Single-Frequency Network) function makes it possible to broadcast the same IP packet from several synchronized eNB entities in the physical multicast channel (PMCH), whose transmission characteristics are identical for all mobiles participating at the MBMS session and for a set of cells. The MBSFN function uses the broadcast transmission mode;

– the SC-PTM (Single-Cell Point-To-Multipoint) function makes it possible to broadcast the same IP packet from a single eNB entity, in the physical downlink shared channel (PDSCH), whose transmission characteristics are specifically

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

defined for each mobile participating at the MBMS session. The SC-PTM function uses the unicast transmission mode.

8.2. Transport architecture

8.2.1. *Functional architecture*

The eMBMS network provides a point to multipoint data transport service, for which unicast or multicast IP packets are transmitted from a source to multiple destinations (Figure 8.1).

This network operates in a broadcast mode, and IP packets of the MBMS session are propagated in a multicast bearer independently of mobile requests.

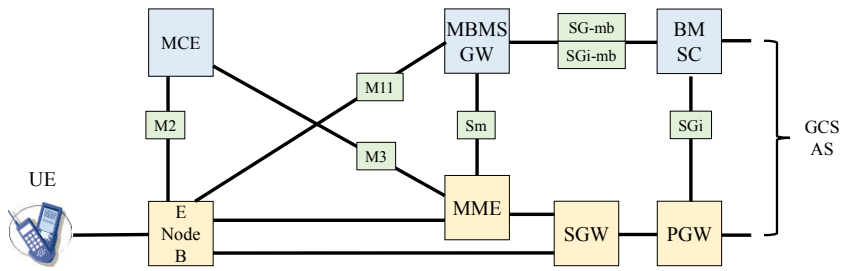

Figure 8.1. *eMBMS network: transport architecture*

The eMBMS network is composed of different areas:

– the MBMS service area, which determines the set of eNB entities which must transmit the MBMS session;

– the MBSFN synchronization area, which determines a set of synchronized eNB entities. The synchronization area is a subset of the service area;

– the MBSFN area, which determines a set of coordinated eNB entities for the simultaneous transmission of an MBMS session. The MBSFN area is a subset of the synchronization area. An eNB entity can belong to several MBSFN areas (up to 8);

– the MBSFN area reserved cells, which determine the eNB entities which are not involved in the transmission of MBSFN sessions.

8.2.1.1. *BM-SC entity*

The broadcast/multicast service center (BM-SC) is the entry point of the service stream in the MBMS network.

The BM-SC entity registers the mobile after the authentication procedure.

This entity announces the start of the MBMS session to the mobiles.

It initiates the procedures of starting, modifying and terminating the multicast bearer.

It attributes a temporary mobile group identity (TMGI) to the session.

It defines the quality of service (QoS) parameters associated with the MBMS session.

It transmits data using the SYNC protocol that ensures synchronization of their delivery through a set of eNB entities.

8.2.1.2. *MBMS GW entity*

The MBMS gateway (GW) can be implemented in specific equipment or be integrated with BM-SC or SGW entities.

The MBMS GW entity allocates an IP multicast address to the bearer for the delivery of data to eNB entities.

This entity is involved in the procedures of starting, modifying and terminating the multicast bearer.

8.2.1.3. *MCE*

The multi-cell/multicast coordination entity (MCE) determines the operating mode of the radio interface, MBSFN or SC-PTM.

The MCE may be implemented in specific equipment that controls a set of eNB entities or integrated with the eNB entity.

This entity is involved in the procedures of starting, modifying and terminating the multicast bearer.

It allocates the radio resource to the MBMS session and performs admission control.

It defines the modulation scheme and coding applied to the radio interface.

It performs pre-emption of resources according to the allocation and retention priority (ARP).

It initializes the counting procedure of mobiles involved in the MBMS session.

8.2.2. *Protocol architecture*

The SG-mb interface is the reference point between the BM-SC and MBMS GW entities for signaling via the DIAMETER protocol for starting, modifying or terminating the multicast bearer.

The SGi-mb interface is the reference point between the BM-SC and MBMS GW entities for IP packets corresponding to the MBMS session and SYNC protocol for the synchronization of the eNB entities.

The Sm interface is the reference point between the MBMS GW and MME entities for signaling via the GTPv2-C protocol for starting, modifying or terminating the multicast bearer.

The M3 interface is the reference point between the MME and MCE entities for signaling via the M3-AP protocol for starting, modifying or terminating the multicast bearer.

The M2 interface is the reference point between the MCE and eNB entities for signaling via the M2-AP protocol, for the following functions:

– starting, modifying or terminating the multicast bearer;

– counting of terminals subscribed to an MBMS session;

– configuring the physical channel on the radio interface.

The M1 interface is the reference point between, on the one hand, the MBMS GW entity, and, on the other hand, all eNB entities involved in the distribution of the MBMS session for tunneling traffic, via the GTP-U protocol, corresponding to the IP packet of the MBMS session transmitted in the multicast bearer.

8.3. Service architecture

8.3.1. *Functional architecture*

An MBMS service can be accessed by an entity which proposes a full service to the end user and authorizes him to enable or disable the service. It is usually associated with a short description presented to the end user.

A unit service entity may contain a plurality of separate media objects or streams, which may be provided on various sessions. A session is associated with a unicast bearer or one or more multicast bearers and a set of parameters specifying how content should be received on the mobile side (Figure 8.2).

The authentication infrastructure can be used to enable the establishment of shared keys. Therefore, the infrastructure can provide the authentication service based on the generic bootstrapping architecture (GBA) using the authentication and key agreement (AKA) (Figure 8.2).

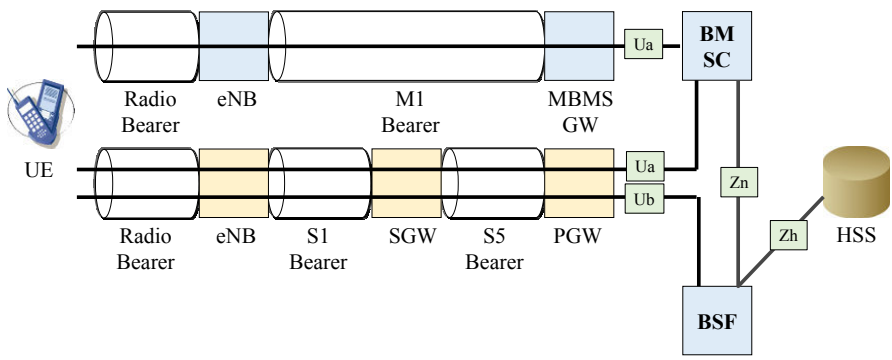

Figure 8.2. *eMBMS network: service architecture*

8.3.1.1. *BSF entity*

The bootstrapping server function (BSF) and the mobile entity must mutually authenticate using the AKA mechanism, and establish on the session keys that are then applied between the mobile and the BM-SC entity.

The home subscriber server (HSS) provides the BSF entity with the cryptographic data calculated from a random (RAND) and the key Ki:

– the seal of the network (AUTN);

– the seal of the mobile (RES);

– the integrity key (IK) and the cipher key (CK). The IK and CK are concatenated to constitute the key Ks.

8.3.1.2. *BM-SC entity*

On mutual authentication, the mobile and the BM-SC entity can execute an application-specific protocol in which message authentication will be based on the session keys generated during the mutual authentication procedure which happens between the mobile and the BSF entity.

The BM-SC entity and the mobile can exchange service and content information on unicast or multicast media from the following functions.

The User Service Discovery/Announcement function provides service description information, which can be provided via the Session and Transmission function or via the Interactive Announcement function (Figure 8.3). This function includes the information needed to initialize the MBMS service.

The Session and Transmission function interacts with the MBMS-GW entity to activate or release the transmission resources (Figure 8.3).

The Session and Transmission function is further subdivided into the sub-functions MBMS Delivery and Associated Delivery.

The MBMS Delivery sub-function structures the data transmitted by the BM-SC entity to the mobile, in IP unicast or multicast packets:

– the data is optionally protected (encryption and/or integrity check);

– the data is optionally protected by a forward error correction (FEC).

The Associated Delivery sub-function is invoked by the mobile, in connection with the transmission of data for the following cases:

– the file repair to complete the missing data;

– the verification of the delivery of data and collection of statistics.

The Key Management function is subdivided into the sub-functions Key Request and Key Distribution (Figure 8.3).

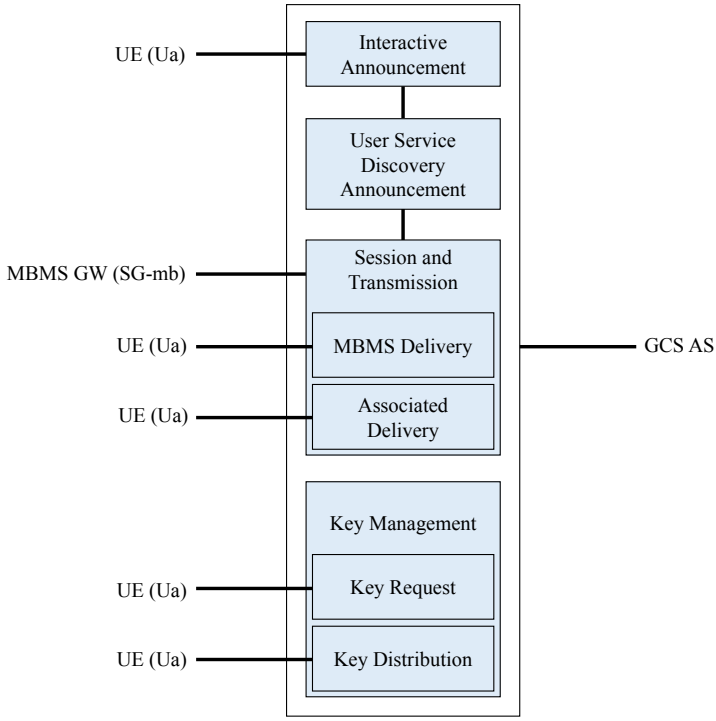

Figure 8.3. *Structure of the BM-SC entity*

The Key Request sub-function retrieves a key derived from the key Ks from the BSF entity and deduces the following keys (Figure 8.4):

– the MBMS Request Key (MRK) used for mutual authentication between the mobile and the BM-SC entity;

– the MBMS User Key (MUK) transmitted to the sub-function Key Distribution.

The Key Distribution sub-function generates two keys, the MBMS service key (MSK) and the MBMS traffic key (MTK) (Figure 8.4).

The MTK is used to protect the data exchanged between the mobile and the BM-SC entity.

The MSK protects the transmission of the MTK to the mobile (Figure 8.4).

The MUK protects the transmission of the MSK to the mobile (Figure 8.4).

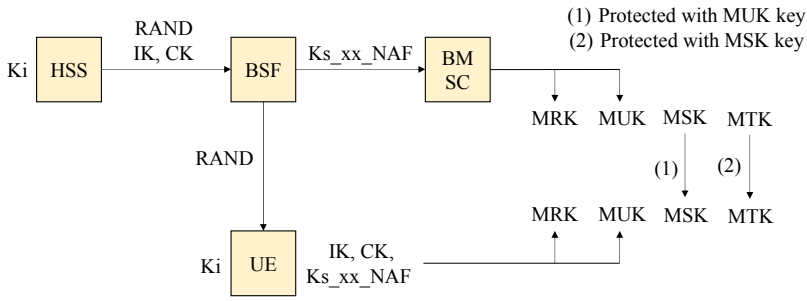

Figure 8.4. *Setting up the keys*

8.3.2. *Protocol architecture*

The Ub interface is the reference point between the mobile and the BSF entity, for mutual authentication, via the hypertext transfer protocol (HTTP).

The Ua interface is the reference point between the mobile and the BM-SC entity, for data relating to the following functions (Figure 8.5):

– User Service Discovery/Announcement, via HTTP or FLUTE (File Delivery over Unidirectional Transport);

– MBMS Delivery, via the real-time transport protocol (RTP) for voice and video (streaming) or via FLUTE for downloading files;

– Associated Delivery, via HTTP or FLUTE;

– Key Request, via HTTP;

– Key Distribution, via MIKEY (*Multimedia Internet KEYing*).

The Zh interface is the reference point between the BSF and HSS entities, via DIAMETER, for the transfer of the cryptographic data.

The Zn interface is the reference point between the BSF and BM-SC entities, via DIAMETER, for the recovery of the key Ks_xx_NAF, derived from the key Ks.

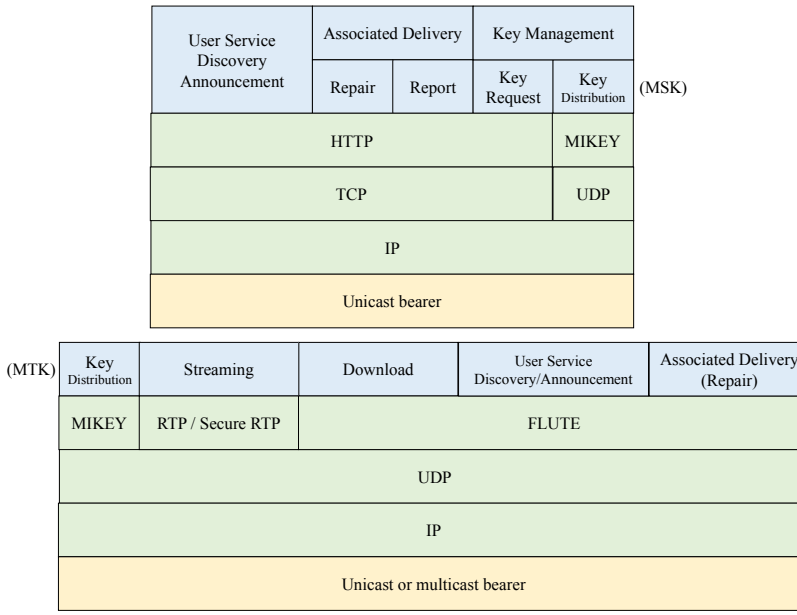

Figure 8.5. *Protocol architecture of the Ua interface*

8.4. Radio interface

In the MBSFN mode, the PMCH transmits the multicast channel (MCH) that multiplexes the multicast control channel (MCCH) and multicast traffic channel (MTCH).

The MCCH is a unidirectional logical channel that is used to transmit RRC (Radio Resource Control) messages for control information associated with IP packets transmitted in the broadcast mode.

The MTCH is a unidirectional logical channel that is used to transmit the IP packets, relating to the MBMS application, to the mobile.

In the SC-PTM mode, the SC-MCCH and SC-MTCH are multiplexed in the downlink shared channel (DL-SCH) which is transmitted in the PDSCH.

8.4.1. *MBSFN-RS*

The MBSFN reference signal (RS) is only transmitted over the PMCH to perform the coherent demodulation.

8.4.1.1. *Sequence generation*

The MBSFN-RS is obtained from the following sequence:

$$r_{l,n_s}(m) = \frac{1}{\sqrt{2}}\left(1-2\cdot c(2m)\right) + j\frac{1}{\sqrt{2}}\left(1-2\cdot c(2m+1)\right),$$

$$m = 0,1,\ldots,6N_{\mathrm{RB}}^{\max,\mathrm{DL}} - 1$$

where $N_{\mathrm{RB}}^{\max,\mathrm{DL}}$ is expressed as the number of resource blocks in the frequency domain for the entire bandwidth of the radio channel;

l is the number of the Orthogonal Frequency-Division Multiplexing (OFDM) symbol of the time slot;

n_s is the time slot number of the time frame;

$c(m)$ is a pseudo-random sequence that is 31 bits long.

At the start of every OFDM symbol, the initial c_{init} value of the pseudo-random sequence is obtained with the following formula:

$$c_{\mathrm{init}} = 2^9 \cdot \left(7\cdot\left(n_s+1\right)+l+1\right)\cdot\left(2\cdot N_{\mathrm{ID}}^{\mathrm{MBSFN}}+1\right) + N_{\mathrm{ID}}^{\mathrm{MBSFN}}$$

where $N_{\mathrm{ID}}^{\mathrm{MBSFN}}$ is the identity of the MBSFN.

8.4.1.2. *Mapping to resource elements*

Figure 8.6 describes the mapping to resource elements in the case of a step of 15 kHz between the sub-carriers.

The MBSFN-RS is mapped, in the time domain, to the resource elements located in the third OFDM symbol of an even slot, and in the first and fifth OFDM symbols of an odd slot.

The MBSFN-RS is mapped, in the frequency domain, to the following resource elements:

– even-numbered resource elements for the third OFDM symbol of an even slot and for the fifth OFDM symbol of an odd slot;

– odd-numbered resource elements for the first OFDM symbol of an odd slot.

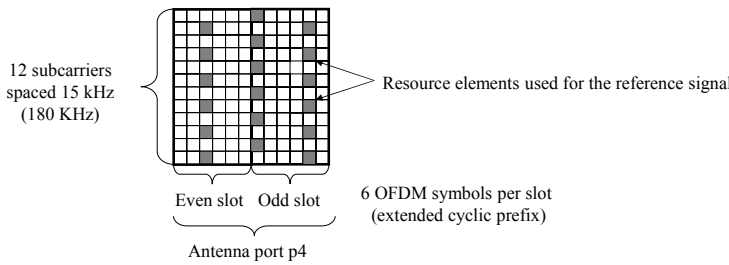

Figure 8.6. *Mapping of the MBSFN-RS: a step of 15 kHz between the sub-carriers*

Figure 8.7 describes the mapping to resource elements in the case of a step of 7.5 kHz between the sub-carriers.

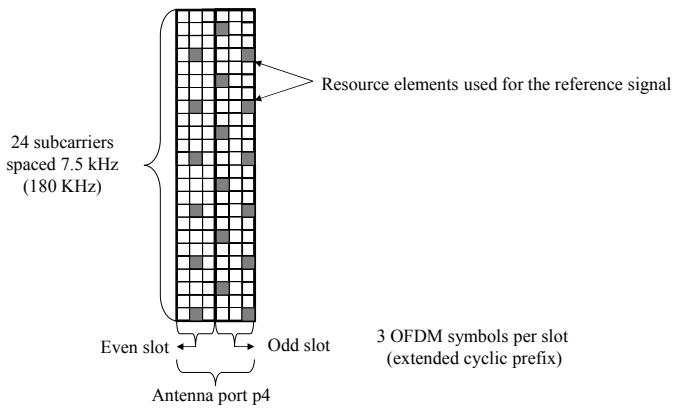

Figure 8.7. *Mapping of the MBSFN-RS: a step of 7.5 kHz between the sub-carriers*

The MBSFN-RS is mapped, in the time domain, to resource elements located in the second OFDM symbol of an even slot, and in the first and the third OFDM symbols of an odd slot.

The MBSFN-RS is mapped, in the frequency domain, to the following resource elements:

– resource elements whose rank is a multiple of 4 for the second OFDM symbol of an even slot and for the third OFDM symbol of an odd slot;

– resource elements whose rank has a two sub-carrier shift for the first OFDM symbol of an odd slot.

8.4.2. *PMCH*

The processing associated with the PMCH is summarized in Figure 8.8.

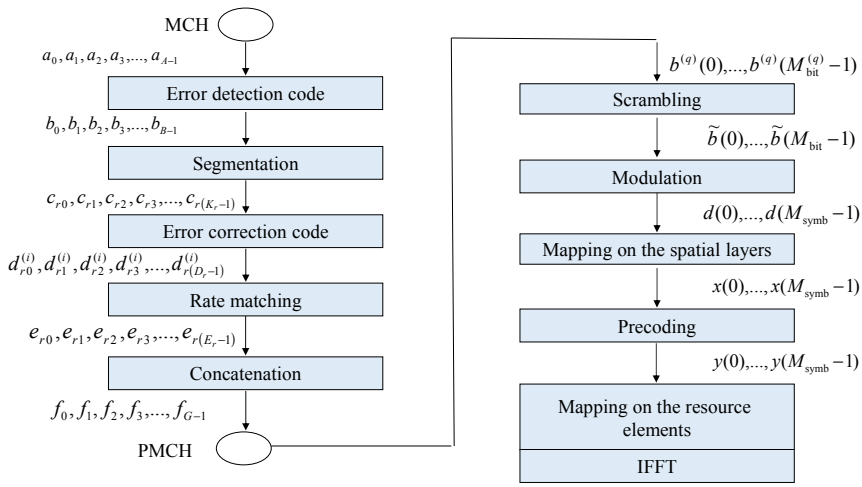

Figure 8.8. *Processing associated with the PMCH*

8.4.2.1. *Error detection codes*

The error detection code is obtained from a cyclic redundancy check (CRC).

The CRC is the remainder when the transport block $a_0, a_1, a_2, a_3, \ldots, a_{A-1}$ is divided by a generator polynomial, whose remainder $p_0, p_1, p_2, p_3, \ldots, p_{L-1}$ constitutes the bits of the CRC.

The concatenation of the transport block $a_0, a_1, a_2, a_3, ..., a_{A-1}$ and of the 24 bits of the cyclic redundancy $p_0, p_1, p_2, p_3, ..., p_{L-1}$ constitute the input structure $b_0, b_1, b_2, b_3, ..., b_{B-1}$ of the segmentation.

8.4.2.2. *Segmentation*

The maximum size of the block processed by the error correction code is equal to 6144 bits.

If the size of the block $b_0, b_1, b_2, b_3, ..., b_{B-1}$ is above this value, it must be segmented; every segment must have its own CRC, the length of which is equal to 24 bits in order to constitute the sequence $c_{r0}, c_{r1}, c_{r2}, c_{r3}, ..., c_{r(K_r-1)}$, where *r and Kr* are respectively the number of segment and the number of bits of the segment.

8.4.2.3. *Error correction code*

When segmentation is performed over the sequence $b_0, b_1, b_2, b_3, ..., b_{B-1}$, the error correction code is applied to each segment.

The error correction code is performed by a turbo code made up by a parallel concatenated convolutional code (PCCC) and by a quadratic permutation polynomial (QPP) interleaving (Figure 8.9).

The error correction code produces three sequences $d_{r0}^{(i)}, d_{r1}^{(i)}, d_{r2}^{(i)}, d_{r3}^{(i)}, ..., d_{r(D_r-1)}^{(i)}$, with $i = 0,1$ and 2, and where D_r is the number of bits of the sequence.

The sequence $d_{r0}^{(0)}, d_{r1}^{(0)}, d_{r2}^{(0)}, d_{r3}^{(0)}, ..., d_{r(D_r-1)}^{(0)}$ is equal to sequence $c_{r0}, c_{r1}, c_{r2}, c_{r3}, ..., c_{r(K_r-1)}$.

The input of the first encoder is the data structure $c_{r0}, c_{r1}, c_{r2}, c_{r3}, ..., c_{r(K_r-1)}$. The sequence $d_{r0}^{(1)}, d_{r1}^{(1)}, d_{r2}^{(1)}, d_{r3}^{(1)}, ..., d_{r(D_r-1)}^{(1)}$ is produced at the output of the first encoder.

The input of the second encoder is the output of the QPP interleaving $c'_0, c'_1, ..., c'_{K-1}$. The sequence $d_{r0}^{(2)}, d_{r1}^{(2)}, d_{r2}^{(2)}, d_{r3}^{(2)}, ..., d_{r(D_r-1)}^{(2)}$ is produced at the output of the second encoder.

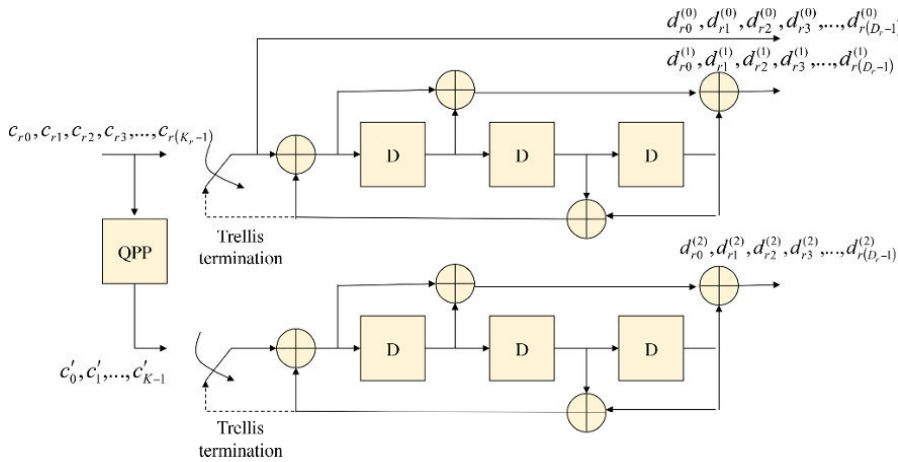

Figure 8.9. *Turbo code*

8.4.2.4. *Rate matching*

The three sequences issued from the turbo code are interleaved and then stored in a circular memory.

The bits of the circular memory are selected or punctured to constitute the output sequence $e_{r0}, e_{r1}, e_{r2}, e_{r3}, \ldots, e_{r(E_r-1)}$, where E_r is the number of bits of the sequence.

8.4.2.5. *Concatenation*

All different sequences $e_{r0}, e_{r1}, e_{r2}, e_{r3}, \ldots, e_{r(E_r-1)}$, with $r = 0, \ldots, C-1$, where C is the number of segments, are concatenated to constitute the sequence $f_0, f_1, f_2, f_3, \ldots, f_{G-1}$, where G is the number of bits of the sequence.

8.4.2.6. *Scrambling*

The sequence of bits $b(0), \ldots, b(M_{\text{bit}}-1)$, M_{bit} that designates the number of bits, is scrambled by the sequence $c(i)$.

This generates the sequence of bits $\tilde{b}(0),...,\tilde{b}(M_{\text{bit}}-1)$, with $\tilde{b}(i)=\left(b(i)+c(i)\right) \bmod 2$.

The scrambling sequence is obtained with a 31-bit long pseudo-random sequence.

The initial value c_{init} of the scrambling sequence is calculated with the following formula:

$$c_{\text{init}} = n_{\text{RNTI}} \cdot 2^{14} + \lfloor n_{\text{s}}/2 \rfloor \cdot 2^{9} + N_{\text{ID}}^{\text{cell}}$$

where n_{RNTI} is the radio network temporary identifier (RNTI), allocated to the mobile during the connection;

n_{s} is the time slot number of the frame;

$N_{\text{ID}}^{\text{cell}}$ is the physical-layer cell identity (PCI).

8.4.2.7. *Modulation*

The sequence of the symbols $d(0),...,d(M_{\text{symb}}-1)$, issued from the quadrature phase-shift keying (QPSK), the 16-quadrature amplitude modulation (16-QAM) or the 64-QAM, is obtained with the sequence of bits $b(0),...,b(M_{\text{bit}}-1)$.

8.4.2.8. *Mapping on the spatial layers*

The PMCH uses a single spatial layer. The set of symbols $d(0),...,d(M_{\text{symb}}-1)$ is mapped in the set $x(0),...,x(M_{\text{symb}}-1)$.

8.4.2.9. *Precoding*

When a single spatial layer is used, no precoding is performed. The set of symbols $x(0),...,x(M_{\text{symb}}-1)$ is mapped in the set $y(0),...,y(M_{\text{symb}}-1)$.

8.4.2.10. *Mapping on the resource elements*

The PMCH occupies all physical resource blocks (PRBs) in the frequency domain, for the duration of a sub-frame.

The PMCH uses an extended cyclic prefix and a 15 kHz or 7.5 kHz step between the sub-carriers.

The control area allocated to the physical control format indicator channel (PCFICH), the physical HARQ indicator channel (PHICH) and the physical downlink control channel (PDCCH) is limited to two OFDM (Orthogonal Frequency-Division Multiplexing) symbols.

The PDCCH is solely used to supply the resources to the mobile for the uplink direction, over the physical uplink control channel (PUCCH).

The control area uses the cyclic prefix defined in the cell for the non-MBSFN sub-frames.

8.4.3. *RRC messages*

8.4.3.1. *Configuration of frames and sub-frames*

The system information block 2 (SIB2) introduces an information element *MBSFN-SubframeConfig* defining sub-frames assigned to the MBMS (Figure 8.10).

```
MBSFN-SubframeConfig
    radioframeAllocationPeriod
    radioframeAllocationOffset
    subframeAllocation
```

radioframeAllocationPeriod: this field contains the value of the frame allocation periodicity to MBMS.

radioframeAllocationOffset: this parameter contains the value of the offset of the frame allocated to MBMS:

SFN mod *radioFrameAllocationPeriod* = *radioFrameAllocationOffset*

subframeAllocation: this parameter defines the sub-frames (among the sub-frames 1, 2, 3, 6, 7, 8) assigned to the MBMS.

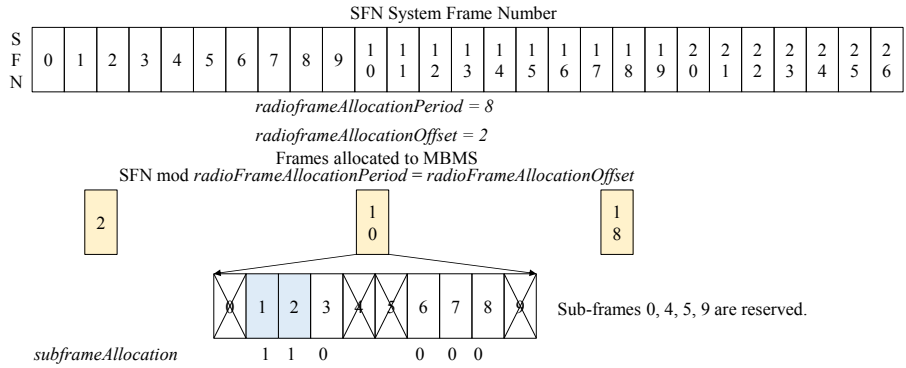

Figure 8.10. *Allocation of frames and sub-frames to the MBMS*

8.4.3.2. *MCCH scheduling*

The SIB13 provides information relating to the MCCH scheduling from the *mcch-Config* information element (Figure 8.11).

```
MCCH Config
    MCCH-RepetitionPeriod
    MCCH-Offset
    MCCH-ModificationPeriod
    sf-AllocInfo
    signallingMCS
```

mcch-RepetitionPeriod: this field defines the repetition period of the MCCH, by number of frames.

mcch-Offset: this field sets the offset value of the frame where the MCCH is located:

SFN mod *mcch-RepetitionPeriod* = *mcch-Offset*

mcch-ModificationPeriod: this field defines the period during which there is no modification of the MCCH. The limits of the period without modification will satisfy the following relationship:

SFN mod *mcch-ModificationPeriod* = *0*

The modification is signaled to the mobile by the downlink control information (DCI) in the 1C format, carried by the PDCCH.

sf-AllocInfo: this field defines the sub-frame where the MCCH is located.

signallingMCS: this field defines the modulation and coding scheme (MCS) applied to data relating to the MCCH.

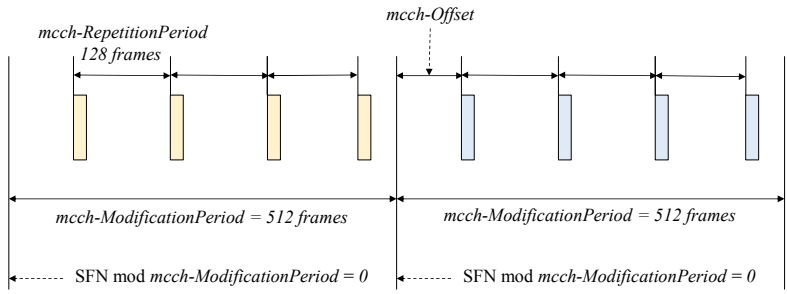

Figure 8.11. *MCCH scheduling*

8.4.3.3. *MTCH scheduling*

Table 8.1 provides the transport of the RRC message that defines the scheduling of the MTCH.

SRB	RLC mode	Logical channel	Transport channel	Physical channel
Not available	UM	MCCH	MCH	PMCH
MBSFNAreaConfiguration				

Table 8.1. *Transport of the RRC message*

The *MBSFNAreaConfiguration* message is transmitted by the eNB entity and contains the following information (Figure 8.12).

```
MBSFNAreaConfiguration
    commonSF-Alloc
    commonSF-AllocPeriod
    PMCH-infolist
```

commonSF-Alloc: this field defines the frames and the sub-frames allocated to each MBSFN area.

commonSF-AllocPeriod: this field defines the periodicity of the allocation pattern of sub-frames common to all MTCHs of the MBSFN area.

PMCH-infolist: this field defines the multiplexing of several MTCHs in each PMCH allocated to an MBSFN area and the MCS applied to the PMCH.

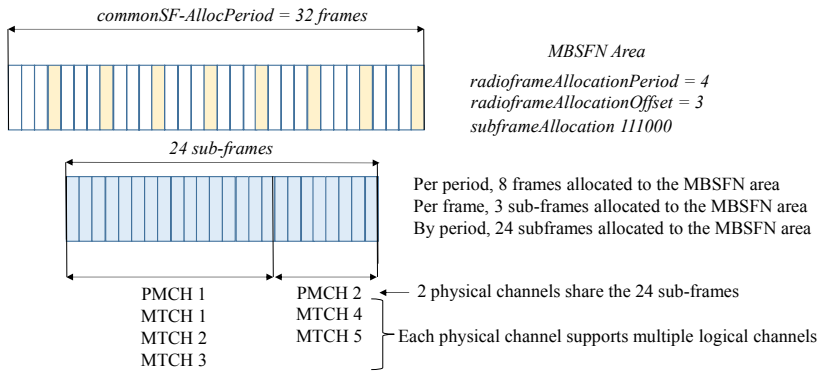

Figure 8.12. *MTCH scheduling*

8.4.3.4. *Counting*

The counting procedure helps the MCE entity to choose the mode of transmission of the MTCH, either the broadcast mode or the unicast mode:

– the unicast mode is most efficient if the number of mobiles subscribed in a program is low. The unicast mode allows the use of the MIMO (Multiple Input Multiple Output) transmission and optimization of the modulation and the coding scheme;

– the broadcast mode is more efficient if the number of mobiles subscribed in a program is high. The broadcast mode only transmits a single logical channel regardless of the number of mobiles subscribed in the program.

Table 8.2 provides the characteristics of the message transport relating to counting.

The message *MBMSCountingRequest* is transmitted by the eNB entity and contains a list of programs.

The message *MBMSCountingResponse* is transmitted by each mobile subscribed to one of the programs.

SRB	RLC mode	Logical channel	Transport channel	Physical channel
Not available	UM	MCCH	MCH	PMCH
MBMSCountingRequest				
SRB1	AM	DCCH	UL-SCH	PUSCH
MBMSCountingResponse				

Table 8.2. *Message transport relating to counting*

8.5. Procedures

8.5.1. *Mutual authentication*

Before starting the communication between the mobile and the BM-SC entity, when the mobile does not know if the entity requires the use of shared keys, the mobile can contact the entity for further instructions.

The mutual authentication procedure is described in Figure 8.13.

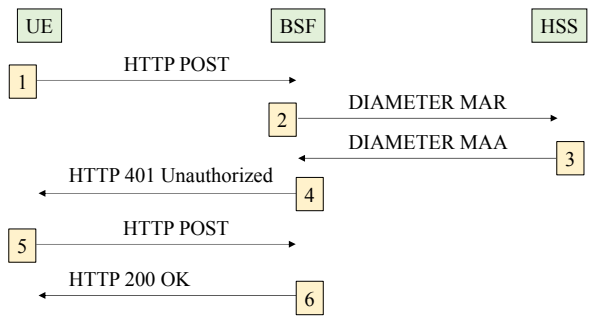

Figure 8.13. *Mutual authentication*

1) The mobile starts the mutual authentication procedure with the BSF entity by sending an HTTP POST request containing its international mobile subscriber identity (IMSI).

2) The BSF entity requests from the HSS entity the cryptographic data (RAND, AUTN, RES, IK, CK) in the message DIAMETER MAR (Multimedia-Authentication-Request).

3) The HSS entity provides the BSF entity with the cryptographic data in the message DIAMETER MAA (Multimedia-Authentication-Answer).

On receipt of the message, the BSF entity generates the keys Ks and Ks_xx_NAF from the keys IK and CK.

4) The BSF entity transmits to the mobile the random (RAND) challenge and the network seal (AUTN) in the message HTTP 401 Unauthorized.

The mobile calculates the cryptographic data from its key Ki and the random (RAND) challenge and compares the calculated network seal with that received.

5) If the result is positive, the mobile sends a new message HTTP POST containing its seal (RES).

On receipt of the message, the BSF entity compares the seals (RES) received from the mobile and the HSS entity.

6) If the result is positive, the BSF entity responds to the mobile with the message HTTP 200 OK containing the lifetime of the key Ks and the bootstrapping transaction identifier (B-TID) built from the RAND challenge and the name of the BSF entity.

8.5.2. *Mobile registration*

Before the communication between the BM-SC entity and the mobile can begin, they must first agree on the use of shared keys obtained during mutual authentication.

The mobile registration procedure is described in Figure 8.14.

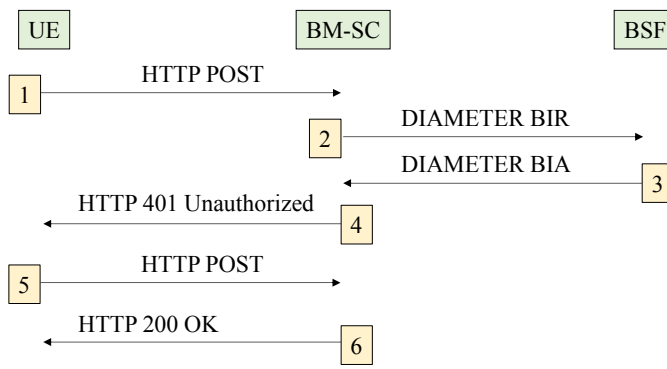

Figure 8.14. *Mobile registration*

1) The mobile transmits to the BM-SC entity the message HTTP POST containing the identifier B-TID and derives the key Ks to generate the MRK and MUK.

2) The BM-SC entity transmits to the BSF entity the message DIAMETER BIR (Bootstrapping-Info-Request) containing the B-TID.

3) On receipt of this message, the BSF entity derives, from the key Ks, the key Ks_xx_NAF it transmits to the BM-SC entity in the message DIAMETER BIA (Bootstrapping-Info-Answer).

On receipt of this message, the BM-SC entity derives the key Ks_xx_NAF to generate the MRK and MUK.

4), 5) and 6) The mobile and BM-SC entity mutually authenticate with the MRK.

8.5.3. *Multicast bearer establishment*

The establishment of the multicast bearer initiates the transmission of a new MBMS session, following the execution of the User Service Discovery/ Announcement function.

The procedure for establishing the multicast bearer is described in Figure 8.15.

1) The procedure is initiated by the BM-SC entity by sending to the MBMS GW entity the message DIAMETER RAR (Re-Auth-Request) containing the characteristics (TMGI, QoS) of the bearer that must be created and the list of the MME entities.

2) The MBMS GW entity responds to the BM-SC entity with the message DIAMETER RAA (Re-Auth-Answer).

3) The MBMS GW entity initiates the construction of the multicast bearer by sending to the MME entity the message GTPv2-C MBMS SESSION START REQUEST containing the IP multicast address of the bearer to create.

4) The MME entity distributes the M3-AP MBMS SESSION START REQUEST message to the multi-cell/multicast coordination entities (MCE), containing the IP multicast address and the characteristics (TMGI, QoS, TEID) of the bearer to create.

5) Each MCE entity responds to the MME entity with the message M3-AP MBMS SESSION START RESPONSE.

6) The MME entity responds to the MBMS GW entity with the message GTPv2-C MBMS SESSION START RESPONSE.

7) The MCE entity sends to the relevant eNB entities the message M2-AP START SESSION REQUEST containing the IP multicast address and the characteristics (TMGI, QoS, TEID) of the bearer to create.

8) The MCE entity simultaneously sends to the relevant eNB entities the message M2-AP SCHEDULING INFORMATION that defines the characteristics of the MTCH.

9) and 10) The eNB entity responds to both messages received with the messages M2-AP SESSION START RESPONSE and M2-AP SCHEDULING INFORMATION RESPONSE.

The eNB entities send the message IGMP JOIN to the IP transport network in order to receive the multicast stream.

11) The eNB entity transmits the MTCH characteristics to the mobiles in the message RRC *MBSFNAreaConfiguration*.

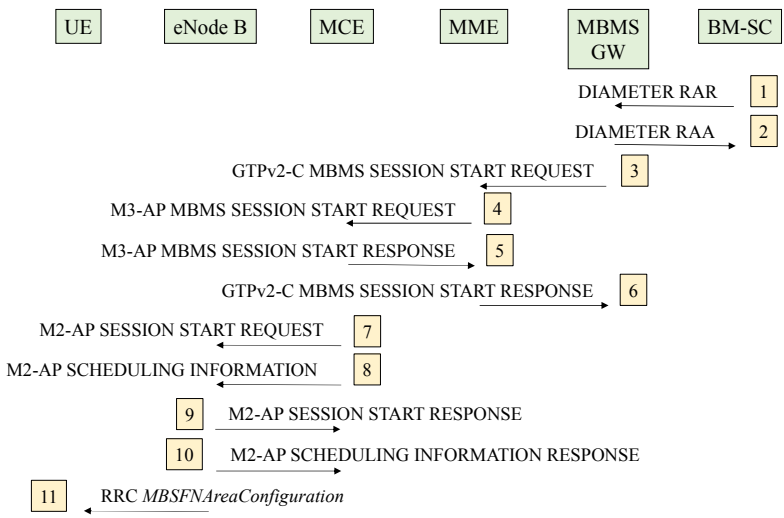

Figure 8.15. *Multicast bearer establishment*

9

LLC Service – GCSE and MCPTT Functions

9.1. Introduction

The provision of a group communication service is achieved through the introduction of two complementary functionalities, one called the group communication system enablers (GCSE) and the other the mission critical push to talk (MCPTT).

The separation of two features has been chosen to flexibly accommodate the operational needs of group communication services that should be different for different types of user groups.

The GCSE function allows mobile devices to participate in group communication for multiple groups in parallel, which can be one or more voice, video or data communications. This feature resides in the mobile and in a GCS application server that determines how these communications will be handled.

The MCPTT function manages group interactions such as floor control, which decides which of the mobiles that have issued a communication request is allowed to communicate, or mechanisms to join or leave a group communication in course, or creating, editing and deleting groups.

The MCPTT function operates on mobiles with radio coverage provided by the evolved universal terrestrial radio access network (E-UTRAN), and also on mobiles using a proximity service (ProSe) sidelink, without impact on the evolved packet system (EPS) or on mobiles running as ProSe relays.

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

9.2. GCSE function

9.2.1. *Functional architecture*

The GCS application server supports the following functions (Figure 9.1):

– signaling exchanged via the GC1 interface with the mobile;

– delivery of the downlink data to a group of mobiles using multicast transmission of the evolved multimedia broadcast/multicast service (eMBMS), via the MB2-U interface with the broadcast/multicast service center (BM-SC);

– reception of the uplink data, using the unicast transmission of the EPS network, via the SGi interface with the PDN gateway (PGW);

– management of multicast transmission via the MB2-C interface with the BM-SC entity;

– bidirectional exchange of data, using the unicast transmission of the EPS network, via the SGi interface with the PGW entity;

– session management, via the Rx interface with the policy and charging rules function (PCRF);

– support for service continuity allowing the mobile to switch between unicast transmission and multicast transmission.

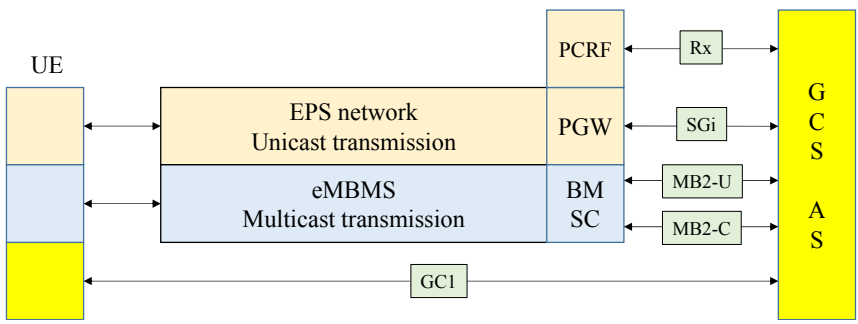

Figure 9.1. *GCSE function*

For multicast transmission, the GCS application server uses the MB2-C interface to indicate the QCI (QoS Class Identifier) priority level applied to the flow (Table 9.1).

For unicast transmission, the GCS application server uses the Rx interface to indicate the QCI priority level applied to the flow (Table 9.1).

QCI	Resource type	Priority	Delay	Error rate	Services
65	GBR	0.7	75 ms	10^{-2}	Voice service Critical mission
66		2	100 ms	10^{-2}	Voice service Non-critical mission
69	Non-GBR	0.5	60 ms	10^{-6}	Telephone signaling Critical mission
70		5.5	200 ms	10^{-6}	Data Critical mission

Table 9.1. *QoS class identifier*

9.2.2. *Protocol architecture*

The GC1 interface is defined as part of the MCPTT function.

The MB2 interface provides access to the eMBMS service support from a GCS application server.

It carries the control plane signaling (MB2-C) and the traffic plane flow (MB2-U) between the GCS server and the BM-SC entity.

The MB2 interface has the following properties:

– the MB2 interface is used by the GCS application server to interact with the BM-SC entity for managing eMBMS bearers;

– the GCS application server can use the service of several BM-SC entities, each with a separate interface;

– the BM-SC entity can provide services to several GCS application servers via a separate MB2 interface;

– an eMBMS session is supported by a single BM-SC entity and is provided to a single GCS application server;

– the information describing the user plane (IP address and UDP port for destination side), for data stream transmission on the MB2-U interface, must be exchanged via the MB2-C interface.

The MB2-C interface is the reference point between the BM-SC entity and the GCS application server. This interface supports the DIAMETER protocol.

The message DIAMETER GAR (GCS-Action-Request) allows the GCS application server to request an allocation of a temporary mobile group identity (TMGI) or an activation of the multicast bearer.

The message DIAMETER GAA (GCS-Action-Answer) is the response of the BM-SC entity to the GAR message.

The message DIAMETER GNR (GCS-Notification-Request) allows the BM-SC entity to send a status notification of the TMGI or the multicast bearer.

The message DIAMETER GNA (GCS-Notification-Answer) is the response of the GCS application server to the GNR message.

9.3. MCPTT function

9.3.1. *Functional architecture*

The MCPTT function uses the multimedia service provided by the IP multimedia sub-system (IMS), the proximity service, the group communication service provided by the eMBMS and the data transfer provided by the EPS.

The MCPTT function is composed of two parts providing, respectively, the application services and the management services.

The application services are related to the mobile registration, the session establishment, the media negotiation, the distribution and the media mixer, as well as the floor control.

The management services are related to the group management, the configuration, the identity and the keys.

9.3.1.1. *Application services*

Application services are provided by the MCPTT server, which is also an instantiation of the GCS application server, in order to control multicast and unicast transmissions for group communications (Figure 9.2).

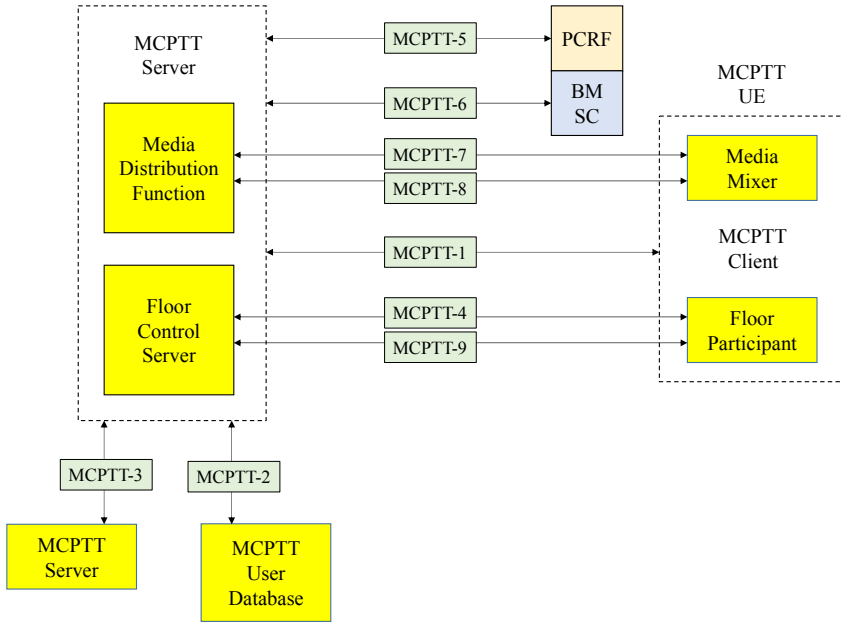

Figure 9.2. *Application services*

Assuming the role of a GCS application server, the MCPTT server is responsible for the following functions:

– keeping track of the mobile location with regard to the availability of the multicast service;

– requesting the allocation of resources to the BM-SC entity for transmission using the eMBMS network;

– announcing the association of multicast resources with calls;

– determining for each MCPTT mobile involved in a given call whether to use the unicast or multicast transmission;

– informing the media distribution function for flows requiring support.

The MCPTT server acting as control is responsible for the following functions:

– the call control, such as the application of rules for participation in group calls;

– the interface with the group management server for the group policy and affiliation status information of the users served by this server;

– the entity of the floor control management in a group call and a private call;

– the management of the media processing entity (conference, transcoding).

The MCPTT server acting as participant is responsible for the following functions:

– the call control, for example, authorization to participate in group calls;

– the support of group affiliation for the MCPTT user, including enforcement of the maximum number of simultaneous group affiliations;

– the relay of the call control and floor control messages between the MCPTT client and the MCPTT server acting as a control;

– the media processing for its users (transcoding, recording, legal interception) for both unicast and multicast flows.

9.3.1.2. *Management services*

The mobile receives an initial configuration via a boot procedure that provides the various clients (MCPTT client, group management client, configuration management client, identity management client, key management client) with the necessary information when connecting to the MCPTT function. This includes PDN connection information and identity information for all servers with which the mobile must interact.

The configuration management provides the following information: user data, user profile data, service configuration data and group configuration data (Figure 9.3).

The user data sets the maximum number of simultaneous group calls and private calls when the mobile is under the coverage of the 4G network or out of coverage.

The user profile data is stored in the MCPTT database. The configuration management server is used to configure user profile data in MCPTT mobiles. The MCPTT server obtains the user profile data from the MCPTT database (Figure 9.3).

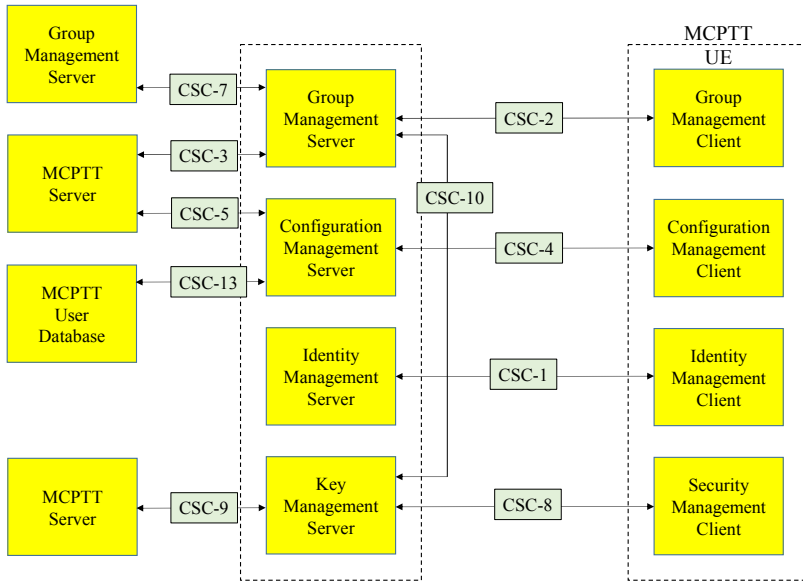

Figure 9.3. *Management services*

The user profile data sets authorizations to initiate and/or receive private calls and group calls.

The service configuration data is stored on the MCPTT server. The configuration management server is used to configure MCPTT mobiles (Figure 9.3).

The service configuration data defines the parameters (timers) associated with the different types of calls (group call, private call) and the floor control.

The group configuration data is stored in the group management server that configures the MCPTT mobile and the MCPTT server (Figure 9.3).

The group configuration data is for the rules to be used for media mixing and for the group call when the mobile is under coverage of the 4G network or out of coverage.

The group management allows the group to be created by the administrator and the user group by an authorized user or by the dispatcher. Group grouping allows dispatchers or authorized users to temporarily combine different groups (Figure 9.3).

The MCPTT mobile requires a token that allows access to different servers. The identity management client must be authenticated by the identity management server that provides the authorization token (Figure 9.3).

When an MCPTT client is granted access to the MCPTT domain, it can obtain the key associated with the user's identity using the authorization token.

The identity keys are required to support key distribution for SIP signaling, floor control and data. The key management server provides the identity keys to the key management client, the group management server and the MCPTT server (Figure 9.3).

The key distribution for signaling and floor control is performed by the MCPTT client that sends the key to the MCPTT server.

The group key distribution is performed by the group management server that sends the group key to the different MCPTT clients. The group management server may distribute the group key to the MCPTT server to enable use of the media mixer function.

In the case of a private call, the key distribution is performed by the mobile that initializes the call.

9.3.2. *Protocol architecture*

9.3.2.1. *Application services*

Since the MCPTT server assumes the functions of the GCS AS server, the MCPTT-1 interface corresponds to the GC1 reference point.

The MCPTT-1 interface is the reference point between the MCPTT client and the MCPTT server. The MCPTT-1 interface supports signaling for establishing a session.

The MCPTT-1 interface uses SIP-1 and SIP-2 reference points for the transport and the routing of the session initiation protocol (SIP). The MCPTT-1 interface can use the HTTP-1 and HTTP-2 reference points (Figure 9.4).

The MCPTT-1 interface may provide the MCPTT server with location information (E-UTRAN cell global identifier (ECGI)), in order to verify the availability of multicast service for the MCPTT client.

The MCPTT-1 interface also allows the provision of the TMGI to the mobile.

The messages supported on this interface may also include information describing the mapping of transport resources to specific group calls.

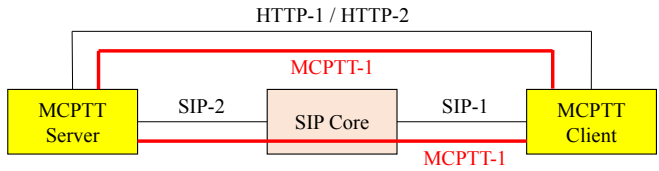

Figure 9.4. *MCPTT-1 interfaces*

The MCPTT-2 interface is the reference point between the MCPTT server and the MCPTT database, via the DIAMETER protocol, to retrieve information about a specific user.

The MCPTT-3 interface is the reference point between MCPTT servers. The MCPTT-3 interface uses the SIP-2 reference point or SIP-2 and SIP-3 reference points for the transport and the routing of SIP signaling (Figure 9.5).

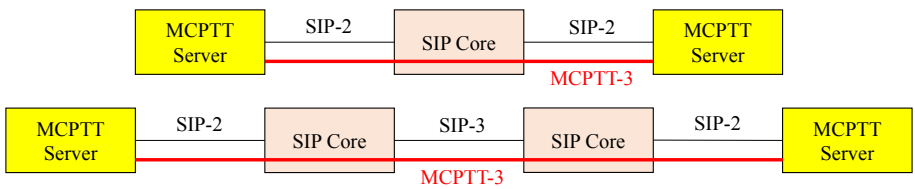

Figure 9.5. *MCPTT-3 interfaces*

The MCPTT-4 interface is the reference point between the floor control server and the floor control client, for the signaling transmitted on unicast support. The MCPTT-4 interface uses the SGi reference point.

Since the MCPTT server assumes the functions of the GCS AS server, the MCPTT-5 interface corresponds to the Rx reference point.

The MCPTT-5 interface is the reference point between the media distribution function and the PCRF entity, in order to obtain the QoS parameters of the bearer.

Since the MCPTT server assumes the functions of the GCS AS server, the MCPTT-6 interface corresponds to the MB2-C reference point.

The MCPTT-6 interface is the reference point between the MCPTT server and the BM-SC entity for the activation of the multicast bearer.

The MCPTT-7 interface is the reference point between the media distribution function and the media mixer, for unicast media exchange. The MCPTT-7 interface uses the SGi reference point.

The MCPTT-8 interface is the reference point between the media distribution function and the media mixer, for multicast media transfer. The MCPTT-8 interface uses the MB2-U reference point.

The MCPTT-9 interface is the reference point between the floor control server and the floor control client, for the signaling transmitted on the multicast support. The MCPTT-9 interface uses the MB2-U reference point.

9.3.2.2. *Management services*

The CSC-1 interface is the reference point between the server and the client performing the identity management.

The CSC-2 interface is the reference point between the server and the client performing the group management.

This interface uses SIP-1 and SIP-2 reference points for the transport and the routing of subscription-related signaling, and HTTP-1 and HTTP-2 reference points for the transport and the routing of signaling not related to the subscription.

The CSC-3 interface is the reference point between the server performing the group management and the MCPTT server.

This interface uses the SIP-2 reference point for the transport and the routing of subscription-related signaling, and the HTTP-1 and HTTP-2 reference points for the transport and the routing of signaling not related to the subscription.

The CSC-4 interface is the reference point between the server and the client performing the configuration management.

This interface uses SIP-1 and SIP-2 reference points for the transport and the routing of subscription-related signaling, and HTTP-1 and HTTP-2 reference points for the transport and the routing of signaling not related to the subscription.

The CSC-5 interface is the reference point between the server performing the configuration management and the MCPTT server.

This interface uses the SIP-2 reference point for the transport and the routing of subscription-related signaling, and the HTTP-1 and HTTP-2 reference points for the transport and the routing of signaling not related to the subscription.

The CSC-7 interface is the reference point between the servers performing the group management.

This interface uses SIP-2 and SIP-3 reference points for the transport and the routing of subscription-related signaling, and HTTP-1, HTTP-2 and HTTP-3 reference points for the transport and the routing of signaling not related to the subscription.

The CSC-8 interface is the reference point between the server and the client performing the key management. The CSC-8 interface uses the HTTP-1 and HTTP-2 reference points.

The CSC-9 interface is the reference point between the server performing the key management and the MCPTT server. The CSC-9 interface uses the HTTP-1 and HTTP-2 reference points.

The CSC-10 interface is the reference point between the servers performing, on the one hand, the key management and, on the other hand, the group management. This interface uses the HTTP-1, HTTP-2 and possibly HTTP-3 reference points.

The CSC-11 interface is the reference point between the server and the client performing the sidelink configuration management when the mobile is out of coverage. This interface uses HTTP-1 and HTTP-2 reference points.

The CSC-12 interface is the reference point between the server and the client performing the sidelink group management, when the mobile is out of coverage. This interface uses the HTTP-1 and HTTP-2 reference points.

The CSC-13 interface is the reference point between the server performing the configuration management and the user's database.

9.3.2.3. *Signaling transport*

The signaling exchanged for the application services on the MCPTT-x interfaces and the management services on the CSC-x interfaces is carried by the SIP and HTTP protocols.

The SIP-1 interface is the reference point between the SIP client (the mobile) and the SIP core. This interface allows mobile registration, event subscription and notification, TMGI communication, session establishment and media negotiation.

The SIP-2 interface is the reference point between the SIP application server (MCPTT function) and the SIP core. This interface makes it possible to inform the application server about the mobile activities: registration, event subscription and notification, the TMGI communication, session establishment and media negotiation.

The SIP-3 interface is the reference point between SIP cores. This interface allows event subscription and notification, session establishment and media negotiation.

The HTTP-1 interface is the reference point between the HTTP client (the mobile) and the HTTP proxy server.

The HTTP-2 interface is the reference point between the HTTP server (MCPTT function) and the HTTP proxy server.

The HTTP-3 interface is the reference point between HTTP proxy servers.

9.4. Procedures

9.4.1. *Group creation*

The procedure for creating a group is depicted in Figure 9.6.

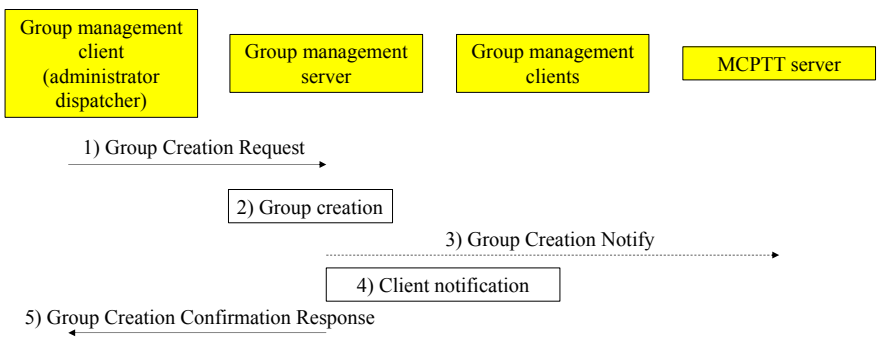

Figure 9.6. *Group creation*

1) The group management client (administrator, dispatcher), authorized to create a group, sends a request to the group management server. User identities must be included in this message.

2) When creating the group, the group management server creates and stores the group information from the group configuration data. The group management server checks the maximum limit of the total number of members of the MCPTT group.

3) The group management server can notify the MCPTT server for the group creation with the information of the group members.

4) The MCPTT group members are informed by the group management server of the new configuration data of the group.

5) The group management server confirms the group creation to the group management client (administrator, dispatcher) that initialized the request.

9.4.2. *Group affiliation*

The group affiliation procedure is described in Figure 9.7.

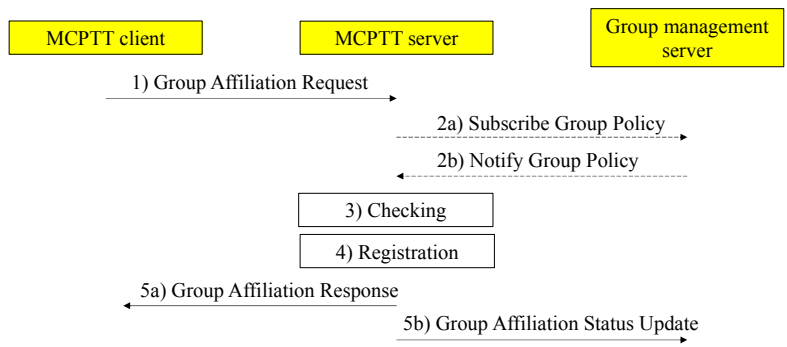

Figure 9.7. *Group affiliation*

1) The MCPTT client requests the MCPTT server to join an MCPTT group or a set of MCPTT groups. The MCPTT client must provide their MCPTT identifier and MCPTT group identifier(s).

2) The MCPTT server checks whether the group rule is cached locally. In the opposite case, the MCPTT server requests the group rule from the group management server (2a). The MCPTT server receives group rule from the group management server (2b).

3) Depending on the group rule and the user's subscription, the MCPTT server checks whether the MCPTT group is enabled and whether the MCPTT client is allowed to join the requested MCPTT group or not. The MCPTT server also checks the maximum limit of the total number of MCPTT groups that the user can be affiliated with at the same time.

4) If the MCPTT client is allowed to join the requested MCPTT group(s), the MCPTT server registers the user's affiliation status for the requested MCPTT group(s).

5) The MCPTT server confirms the affiliation to the MCPTT client (5a) and updates the group management server with the user's affiliation status for the requested MCPTT group (5b).

9.4.3. *Session pre-establishment*

The session pre-establishment is a procedure between the MCPTT client and the MCPTT server in order to exchange the parameters necessary for bearer description. Once the pre-established session is complete, the bearer of the floor control messages is still active.

The MCPTT client is able to activate the voice bearer at any time:

– immediately after the pre-established session procedure;

– using SIP signaling when an MCPTT call is initiated.

The session pre-establishment procedure concerns different types of calls:

– group calls;

– private calls;

– group emergency calls;

– group calls in case of imminent danger;

– private emergency calls;

– emergency alerts.

The session pre-establishment procedure is described in Figure 9.8.

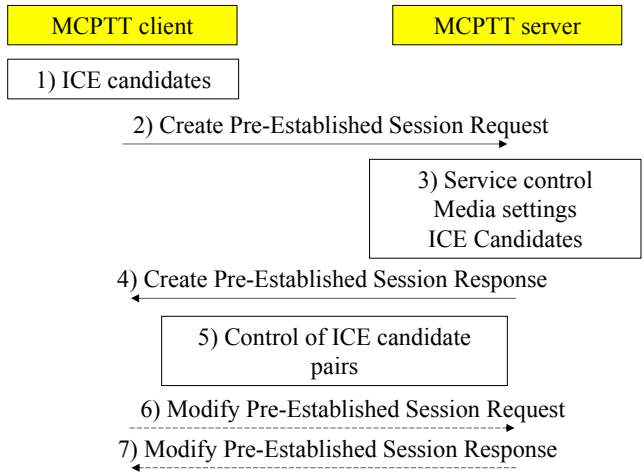

Figure 9.8. *Session pre-establishment: group call*

1) The MCPTT client brings together ICE (Interactive Connectivity Establishment) candidates. The ICE mechanism is used for traversing network address translation (NAT) for SIP messages and voice streams.

2) The MCPTT client sends a request to the MCPTT server to create a pre-established session.

3) The MCPTT server performs the necessary service check, obtains the media parameters, for example by interacting with the media distribution function, and gathers the ICE candidates.

4) The MCPTT server sends a pre-established session creation response to the MCPTT client.

5) ICE candidate pair checking takes place, for example, between the MCPTT client and the media distribution function of the MCPTT server.

6) If required, the MCPTT client sends a pre-established session change request to the MCPTT server to update the ICE candidate pair for the pre-established session.

7) The MCPTT server sends a pre-established session response accepting the update of the ICE candidate pair.

9.4.4. *Group call*

The group call is activated when the mobile is under the radio coverage of the 4G network or out of coverage.

The group call is initiated by one of the group members. Initializing a pre-established group call involves inviting all other members affiliated with the group.

The group call procedure is described in Figure 9.9.

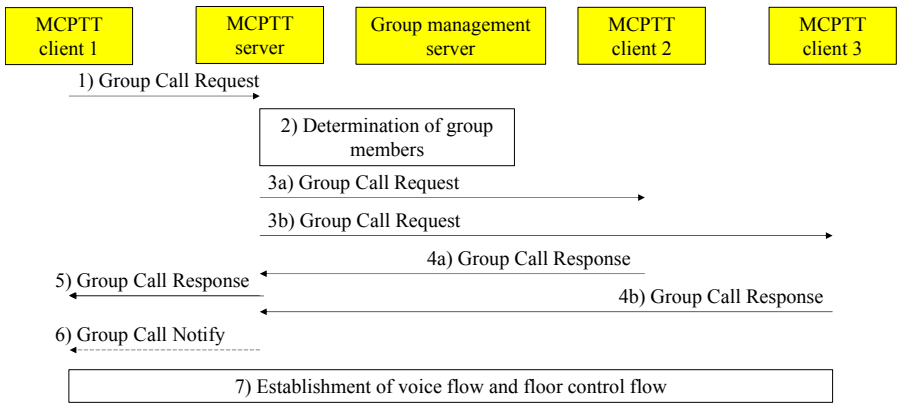

Figure 9.9. *Group call*

1) The MCPTT client 1 sends a group call request to the MCPTT server via the SIP core. The group call request contains the group identifier and the SDP (Session Description Protocol) message containing the media parameters.

2) The MCPTT server verifies that the MCPTT client 1 is authorized to initiate a group call for the selected group.

If allowed and if the group call is in progress for this group, the MCPTT server adds the MCPTT client 1 to the existing MCPTT group call and informs it that the MCPTT group call is already in progress.

Otherwise, the MCPTT server determines the members of this group and their affiliation status based on the information provided by the group management server.

3) The MCPTT server sends the group call request via the SIP core to MCPTT clients affiliated with the group, containing the same media parameters contained in the initial request. The MCPTT server indicates whether an acknowledgment is required for the call or not.

4) The MCPTT clients accept the group call request and a group call response is sent to the MCPTT server. This response may contain an acknowledgment of receipt.

5) The MCPTT server sends the response to the group call, including a selection of the media parameters, to the MCPTT client 1, informing it of the successful completion of the call.

6) If the MCPTT client 1 needs the acknowledgment for the MCPTT affiliate group and the group members do not acknowledge the call establishment, the MCPTT server may continue or give up the call, and then informs the MCPTT client 1.

The MCPTT server may send this notification many times to the MCPTT client 1 during the call when the MCPTT clients join the group call.

7) MCPTT clients have successfully established the user plane for communication and exchange information for the floor.

9.4.5. *Private call*

The private call is activated when the mobile is under the radio coverage of the 4G network or out of coverage.

When the mobile is under the radio coverage of the 4G network, the private call can be with or without floor control. When the mobile is not under the radio coverage, the private call is with a floor control.

The private call can be configured in two start-up modes:

– the automatic start-up mode, in which the establishment of the private call does not require any action on the part of the recipient;

– the manual start-up mode, in which the establishment of the private call requires the recipient to accept or reject the establishment of the call.

The private call procedure for the automatic start-up mode is described in Figure 9.10.

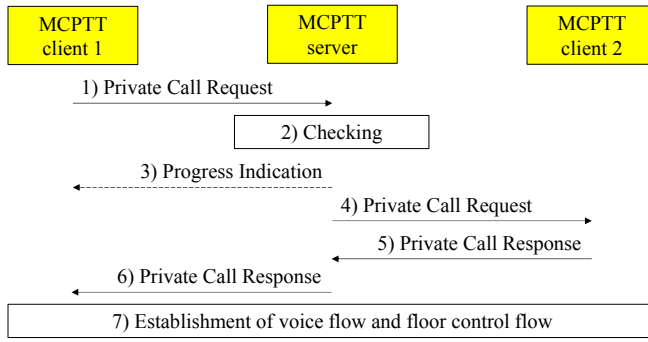

Figure 9.10. *Private call: automatic start-up mode*

1) The MCPTT client 1 sends a private call request to the MCPTT server (via the SIP core). The private call request contains an SDP offer containing one or more types of media. For a private call with floor control, the request also contains an element indicating that the MCPTT client 1 requests the floor.

2) The MCPTT server verifies whether the MCPTT client 1 is authorized to initiate the private call and whether the MCPTT client 2 is authorized to receive the private call. The MCPTT server also checks whether the MCPTT client 1 is authorized to initiate a private call in the automatic start-up mode.

3) The MCPTT server may provide the MCPTT client 1 with an indication of the call setup progress.

4) The MCPTT server sends the private call request to the MCPTT client 2. If the called party has registered with several MCPTT mobiles, the incoming private call request is then delivered only to the designated mobile.

5) The MCPTT client 2 automatically accepts the private call and an MCPTT private call response is sent to the MCPTT server (via the SIP core).

6) The MCPTT server informs the MCPTT client 1 of the successful completion of the private call.

7) MCPTT clients 1 and 2 have established the user plane for communication.

The private call procedure for the manual start-up mode is described in Figure 9.11.

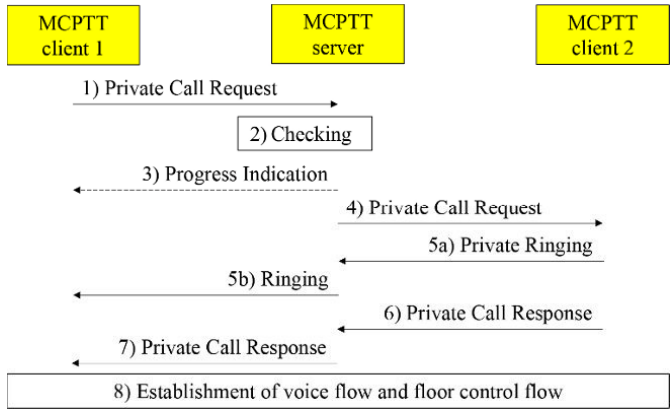

Figure 9.11. *Private call: manual start-up mode*

1) The MCPTT client 1 sends a private call request to the MCPTT client 2 (via the SIP core).

2) The MCPTT server verifies that both MCPTT clients are allowed to establish a private call. The MCPTT server checks whether the MCPTT client 1 is authorized to initiate a call in the manual start-up mode.

3) The MCPTT server sends the private call request to the MCPTT client 2. If the MCPTT client 2 has registered several mobiles to receive the private calls, the MCPTT private call request is then transmitted only to the designated mobiles.

4) The MCPTT server may provide the MCPTT client 1 with an indication of the call setup progress.

5) The MCPTT client 2 sends a ringing indication to the MCPTT server (5a) which transfers it to the MCPTT client 1 (5b).

6) The MCPTT client 2 accepts the call using the manual start-up mode which causes the MCPTT client 2 to send a response to the private call. If the MCPTT 2 user did not accept the incoming call, the MCPTT client 2 sends a call failure response to the MCPTT server without adding the reason for the call failure.

7) The MCPTT server transfers the private call response to the MCPTT client 1.

8) The user plane for communication is established. Each user can transmit media individually.

9.4.6. *Floor*

When the floor control server receives a floor request from a participant, it decides whether or not to grant a resource according to the state of the session, the user's profile and the priority.

When the participant receives a message attributing the floor, they may send media on the previously established uplink bearer.

Some floor control streams can also overlay call control flows to enable efficient call setup and release:

– the call setup request is possibly routed in the request for floor in the uplink or in the information for floor in the downlink;

– the call release request is possibly routed in the request for floor release in the uplink or in the downlink.

The floor procedure is described in Figure 9.12.

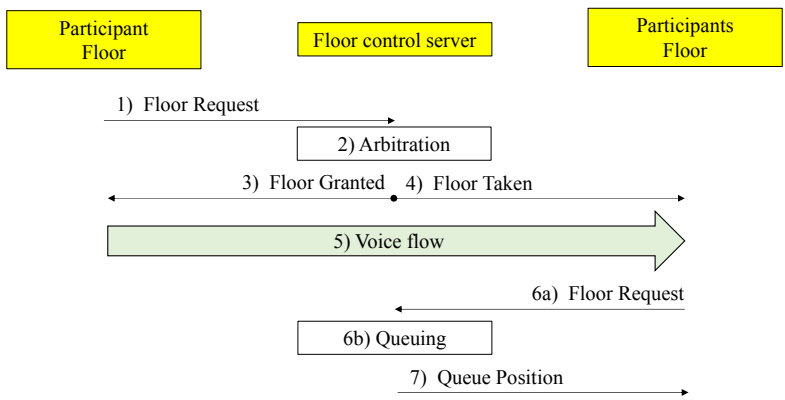

Figure 9.12. *Floor*

1) The participant A wants to send a voice medium during the session. It sends a floor request message to the floor control server which includes the floor priority.

2) The floor control server determines the action (authorization, deny or queuing) to be performed based on criteria (priority, type of participant) and decides to accept the request from participant A. The control server may limit the time during which a participant speaks.

3) The floor control server responds with an allocation message to the participant A, including the maximum allowed time.

4) The floor control server sends a floor message to the different participants.

5) The participant A begins to send a voice flow to the previously established session.

6) If one or more participants request the floor (6a), the request(s) for the floor are queued (6b) according to the decision of the floor control server, for example depending on the floor priority.

7) The floor control server sends information about the queue position to the participants.

10

MTC Service – Network Architecture

10.1. Functional architecture

The term CIoT (Cellular Internet of Things) refers to the evolution of the evolved packet system (EPS) for taking into account connected objects.

LTE-M and NB-IoT (NarrowBand Internet of Things) are two technologies whose specificity lies in the radio interface described in Chapter 11.

These two types of radio interfaces use the same network architecture described in Figure 10.1.

The machine type communication (MTC) is performed between an MTC application hosted in the user equipment (UE) and an MTC application hosted in an application server (AS).

The MTC application server can use the services of a services capability server (SCS) to gain access to certain features of the EPS network.

For the direct model, the application server connects directly to the EPS network to establish communications with the terminal using the user plane without using the SCS entity.

For the indirect model, the application server connects indirectly to the EPS network through an SCS entity to use additional MTC services.

For the hybrid model, the application server simultaneously uses the direct model to connect directly to the EPS network in order to establish direct communications and the indirect model using the SCS entity.

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

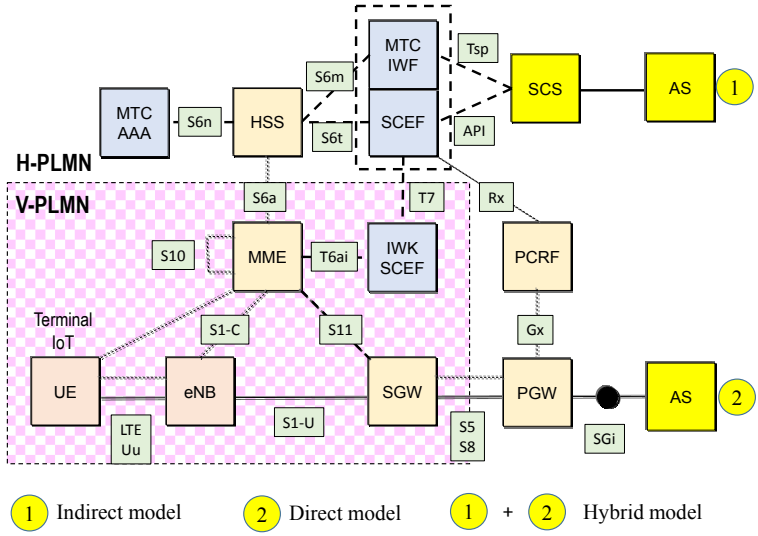

Figure 10.1. *Network architecture*

10.1.1. *MTC-IWF entity*

The MTC-IWF (Interworking) entity hides the internal topology of the EPS network and relays or translates the signaling protocol used on the Tsp interface to invoke specific features of the EPS network.

This entity verifies that the SCS entity is authorized to send a request to trigger the terminal and routes it to the service center which stores the short messages.

It signals to the SCS entity the acceptance or the rejection of the request to trigger the terminal.

It reports to the SCS entity the success or the failure of the short message delivery to the terminal.

It queries the home subscriber server (HSS) for the correspondence between, on the one hand, the E.164 telephone number or an external identifier and, on the other hand, the international mobile subscriber identity (IMSI) of the terminal, and to verify that the SCS entity is authorized to send trigger requests.

10.1.2. *MTC-AAA entity*

The MTC-AAA (Authentication, Authorization and Accounting) entity supports the conversion of the IMSI to external identifiers, in response to a request from the HSS entity.

10.1.3. *SCEF entity*

The service capability exposure function (SCEF) exposes the functionality provided by the EPS network and provides access to EPS network capabilities through application programming interfaces (API).

The services offered by the SCEF entity to the SCS/AS entities are described in the following sections.

10.1.3.1. *Group message delivery*

The group message delivery allows SCS/AS entities to deliver data to a group of devices:

– the delivery of group messages via the evolved Multimedia Broadcast/ Multicast Services (eMBMS);

– the delivery of group messages via unicast transmission of non-IP data delivery (NIDD).

10.1.3.2. *Event monitoring*

Event monitoring is intended to monitor specific events in the EPS network and make this information available to SCS/AS entities.

Event monitoring supports the following functions:

– the monitoring of the association of IMSI and IMEI;

– the accessibility of the terminal;

– the location of the terminal;

– the loss of connectivity;

– the failure of communication;

– the roaming status of the terminal;

– the number of terminals present in a geographical area;

– the availability after failure on the downlink.

10.1.3.3. *High latency communication*

The high latency communication can be used to manage communication with inaccessible devices when they are in a power-saving mode.

This communication is handled by buffering the downlink data in the serving gateway (SGW) or the mobility management entity (MME) until the terminal wakes up.

10.1.3.4. *Session management*

Third-party SCS/AS entities may request that a session be configured with a specific quality of service. This feature is exposed via SCEF entities to SCS/AS entities.

When the SCEF entity receives a request from SCS/AS entities, it forwards the request to the policy and charging rules function (PCRF) via the Rx interface to retrieve the traffic profile.

If the SCEF entity is informed of events occurring in the EPS network via the Rx interface, it reports this to the SCS/AS entities.

10.1.3.4. *Non-IP data delivery*

NIDD support is part of the optimization of the EPS network. The transmission of non-IP data is done by the SCEF entity or via a point-to-point IP tunnel on the SGi interface.

10.1.4. *IWF-SCEF entity*

The IWF-SCEF entity deployed in the visited EPS network allows the terminal in roaming to connect to the SCEF entity located in the home EPS network.

This entity receives the event monitoring reports and sends them to the SCEF entity.

It relays the NIDD between the MME and SCEF entities.

10.2. Network optimization

The optimization of the EPS network is necessary because, on the one hand, the mobiles for the MTC service are characterized by intermittent data transmission at

low bit rate, and, on the other hand, the EPS network is structured for transmissions with high data rates.

Two optimization methods were defined: the first one is based on the control plane (Control Plane CIoT EPS optimization) and the second is based on the user plane (User Plane CIoT EPS optimization) (Figure 10.2).

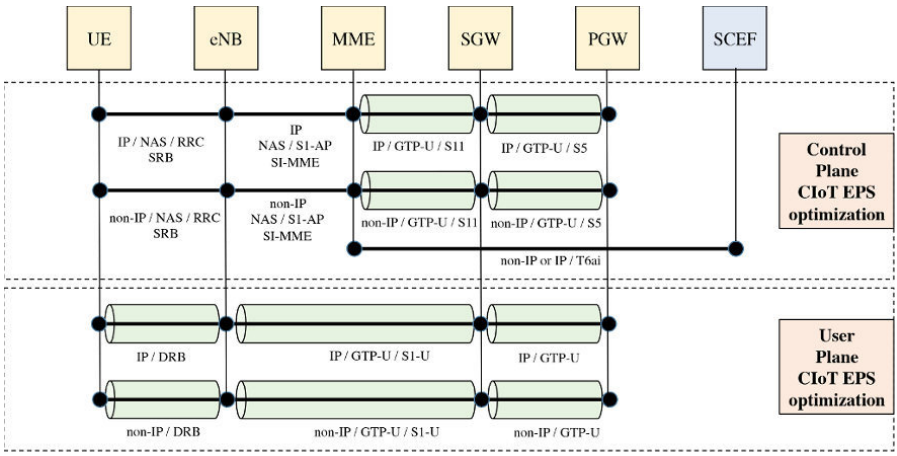

Figure 10.2. *Different variants of data transmission*

In the case of the use of the control plane, the data is carried by the NAS (Non-Access Stratum) messages exchanged between the terminal and the MME entity. This arrangement makes it possible to reduce the number of messages of the control plane during the processing of a session establishment procedure.

Moreover, a new feature allows the terminal to remain connected without having a packet data network (PDN) connection via the SGi interface, since data can be directly transmitted between the MME and SCEF entities. This is useful if a large number of terminals keep the connection idle for a long time and rarely transmit data.

In the case of the use of the user plane, the data are transported in a conventional way. However, the control associated with the maintenance of the bearers introduces two new states of the RRC (Radio Resource Control) connection: the RRC state Suspend and the RRC state Resume.

The RRC state Suspend makes it possible to release the data radio bearer (DRB) and the S1-U bearer while maintaining the context elements. The RRC state Resume allows the bearers to be restored more quickly by optimizing the number of exchanged messages.

10.2.1. *RRC state Suspend*

The procedure for suspending the RRC connection is described in Figure 10.3.

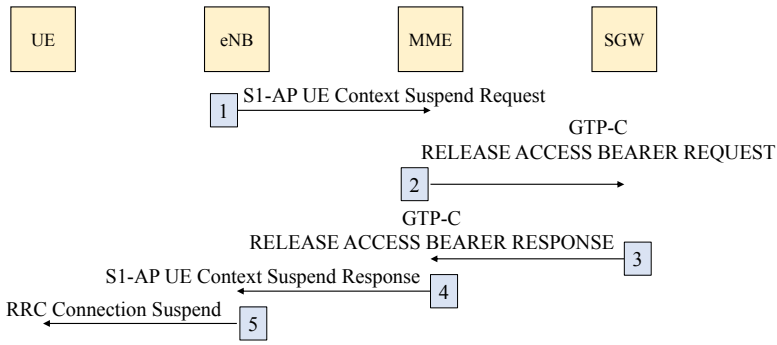

Figure 10.3. *RRC Suspend procedure*

1) The procedure for suspending the RRC connection is initiated by the evolved node base station (eNB) which sends the message S1-AP UE Context Suspend Request to the MME entity.

2) The MME entity transmits the message GTP-C RELEASE ACCESS BEARER REQUEST to the SGW entity.

The SGW removes from the context the information relating to the S1-U bearer (IP address of the eNB entity and the value of the tunnel endpoint identifier (TEID) for the downlink), but retains the other information.

3) The MME entity receives the confirmation of its request in the message GTP-C RELEASE ACCESS BEARER RESPONSE.

The MME entity keeps in its context the parameters relating to the S1-AP connection and the S1-U bearer.

4) The eNB entity receives the confirmation of its request in the message S1-AP UE Context Suspend Response.

The eNB entity keeps in its context the parameters relating to S1-AP and RRC connections.

5) The eNB entity transmits the message RRC Connection Suspend to the terminal which retains in its context the parameters relating to the RRC connection.

10.2.2. *RRC state Resume*

The procedure for resuming the RRC connection is described in Figure 10.4.

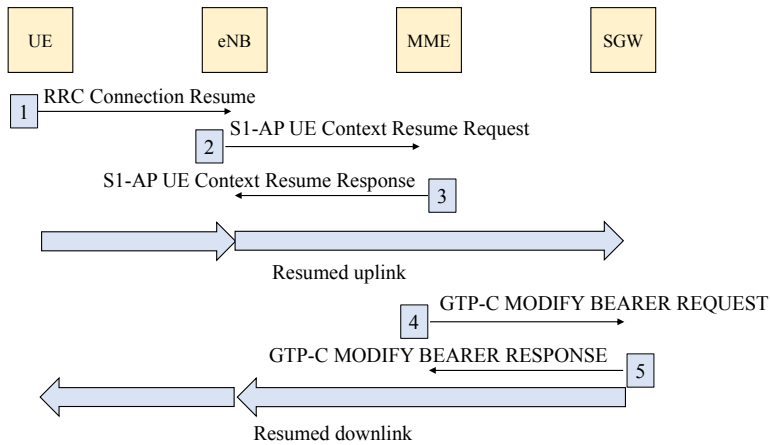

Figure 10.4. *RRC Resume procedure*

1) The procedure for resuming the RRC connection is initialized by the terminal which sends the message RRC Connection Resume to the eNB entity performing a security check.

2) The eNB entity transmits the message S1-AP UE Context Resume Request to the MME entity to warn it of the RRC connection recovery.

3) The MME responds to the eNB entity with the message S1-AP UE Context Resume Response containing the S1-U bearer parameters for uplink recovery.

4) The MME entity transmits to the SGW entity the message GTP-C MODIFY BEARER REQUEST containing the S1-U bearer parameters for downlink recovery.

5) The MME entity receives the confirmation of its request in the message GTP-C MODIFY BEARER RESPONSE.

10.3. Congestion control

Congestion control is useful when multiple terminals simultaneously transmit a connection request to the eNB entity, and an attachment request or a session establishment request to the MME entity.

A terminal can be configured with the low access priority indicator (LAPI) indicating a low priority level.

When the terminal connects, it transmits to the eNB entity an RRC message containing LAPI parameter (Figure 10.5).

When the terminal attaches, it transmits to the MME entity a NAS message containing LAPI parameter (Figure 10.5).

The LAPI is then propagated to SGW and PGW (PDN Gateway) entities in a GTP-C message when establishing bearers (Figure 10.5).

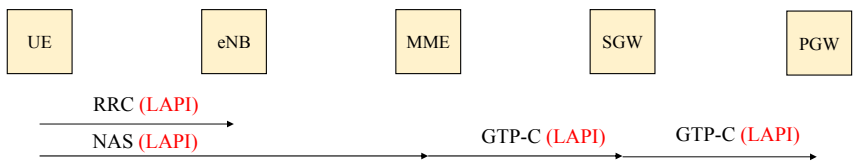

Figure 10.5. *LAPI notification*

The terminal transmits a session establishment request to the MME entity in a NAS message, which triggers the sending of GTP-C messages for bearer creation to the SGW and PGW entities (Figure 10.6).

If the PGW entity has detected congestion, it responds to the SGW entity with a reject GTP-C message, indicating the cause. The SGW entity relays this message to the MME entity (Figure 10.6).

The MME entity indicates to the terminal the reject of the session request in a NAS message containing the cause and value of the retransmission timer (Figure 10.6).

The terminal will have to wait for the timer expiration before retransmitting the session establishment request. The terminal may, however, transmit a session request for another access point name (APN) before the timer expires.

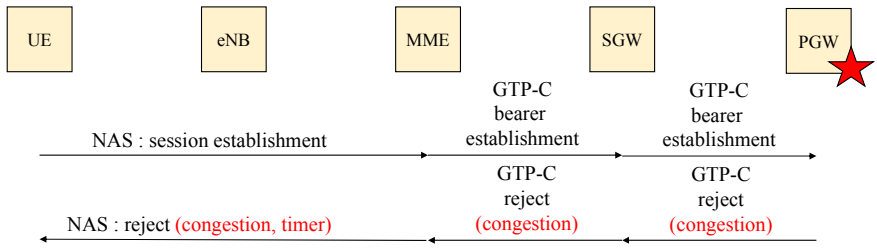

Figure 10.6. *Congestion control: session establishment reject*

If the MME entity detects congestion during an attachment request or location update, it responds to the terminal with a reject NAS message indicating the cause and value of the retransmission timer (Figure 10.7).

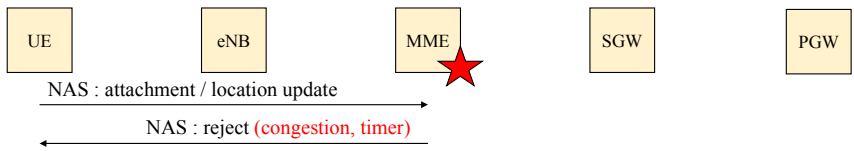

Figure 10.7. *Congestion control: attachment reject*

If the eNB entity detects congestion during a connection request, it responds to the terminal with a reject RRC message indicating the value of the retransmission timer (Figure 10.8).

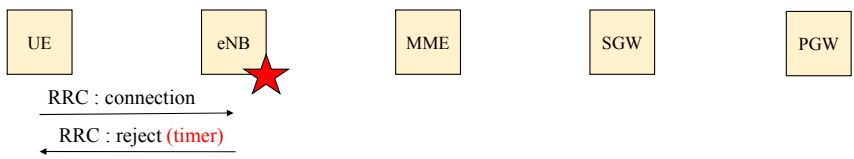

Figure 10.8. *Congestion control: connection reject*

10.4. Procedures

10.4.1. *Triggering procedure*

The triggering procedure allows the SCS entity to send a short message service (SMS) to the terminal. This procedure is used for the indirect model, when the terminal cannot receive an IP packet on the SGi interface (Figure 10.9).

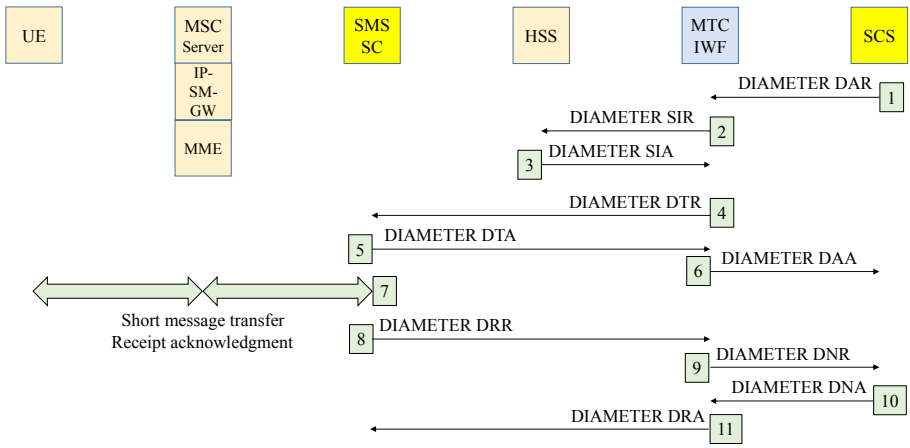

Figure 10.9. *Triggering procedure by short message*

1) The SCS entity transmits the message DIAMETER DAR (Device-Action-Request) to the MTC-IWF entity. This message contains the external identifier or the public identity (MSISDN) of the terminal, the identifier of the SCS entity and the identifier of the MTC application.

2) The MTC-IWF entity sends the message DIAMETER SIR (Subscriber-Information-Request) to the HSS entity to determine whether the SCS entity is authorized to trigger the terminal, in order to resolve the correspondence between the external identifier or the MSISDN and the IMSI.

3) The HSS entity responds with the message DIAMETER SIA (Subscriber-Information-Answer) containing the answers to questions from the MTC-IWF entity, the SMS-SC (Service Center) identity to which the SMS must be routed, and the identity of the next node.

There are three ways to define the identity of the next node:

– the message is routed to the mobile switching center (MSC) server, in the case of the circuit-switched fallback (CSFB) function;

– the message is routed to the IP short-messaging gateway (IP-SM-GW) for accessing the IP multimedia sub-system (IMS);

– the message is directly routed to the MME entity.

4) The MTC-IWF entity transfers the received information to the SMS-SC entity in the message DIAMETER DTR (Device-Trigger-Request).

5) The SMS-SC entity confirms to the MTC-IWF entity in the message DIAMETER DTA (Device-Trigger-Answer) that the sending of the SMS has been accepted.

6) The MTC-IWF entity responds to the SCS entity with the message DIAMETER DAA (Device-Action-Answer), confirming that the request has been accepted.

7) The short message is transmitted to the terminal and is acknowledged to the SMS-SC entity.

8) The SMS-SC entity indicates to the MTC-IWF entity that the SMS has been delivered to the terminal in the message DIAMETER DRR (Device-Report-Request).

9) The MTC-IWF entity indicates to the SCS entity that the SMS has been delivered to the terminal in the message DIAMETER DNR (Device-Notification-Request).

10) The SCS entity acknowledges the receipt of the message DIAMETER DRR with the message DIAMETER DNA (Device-Notification-Answer) transmitted to the MTC-IWF entity.

11) The MTC-IWF entity acknowledges the receipt of the message DIAMETER DRR with the message DIAMETER DRA (Device-Report-Answer) transmitted to the SMS-SC entity.

10.4.2. *Group message delivery*

The group message delivery procedure allows the SCS entity to send a message to multiple terminals using the eMBMS network (Figure 10.10).

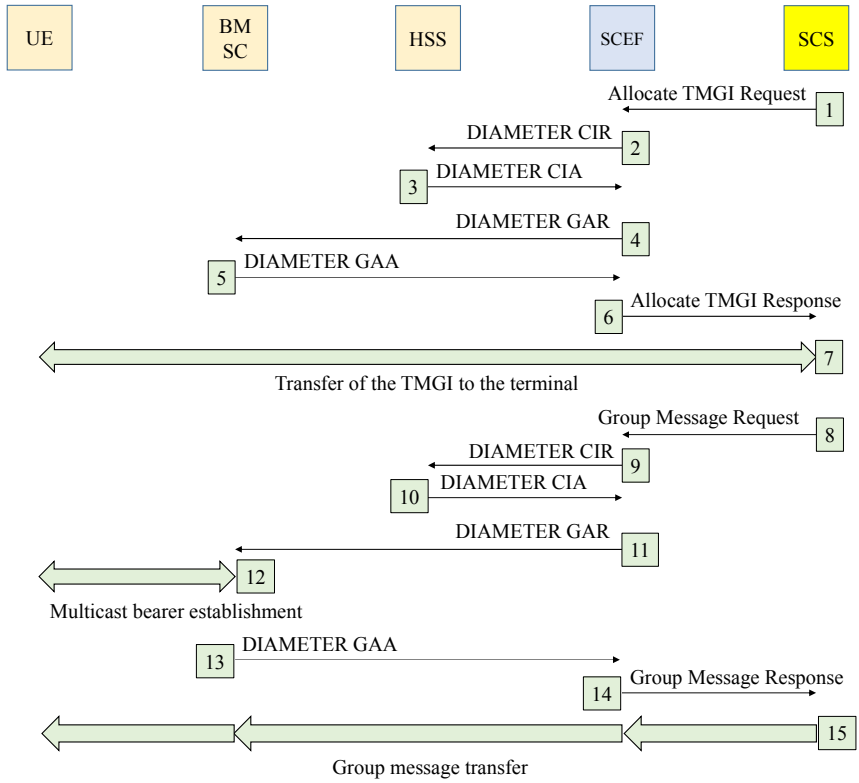

Figure 10.10. *Group message delivery*

1) The SCS entity sends to the SCEF entity a request for allocation of the temporary mobile group identity (TMGI), indicating its identity and the identity of the concerned group. The SCS entity may provide location information (cell identifier list, MBMS service area list, geographic area).

2) and 3) The SCEF entity verifies with the HSS entity whether the SCS entity is allowed to request a TMGI, by the exchange of the messages DIAMETER CIR (Configuration-Information-Request) and CIA (Configuration-Information-Answer).

4) and 5) The SCEF entity retrieves from the broadcast/multicast service center (BM-SC) the TMGI Identifier, by the exchange of the messages DIAMETER GAR (GCS-Action-Request) and DIAMETER GAA (GCS-Action-Answer).

6) The SCEF entity sends the TMGI allocation response to the SCS entity.

7) The terminal retrieves the TMGI from interactions at the application level with the SCS entity.

8) The SCS entity sends to the SCEF entity the group message request containing its identifier, the identifier of the concerned group, the TMGI and optionally, the location information and the start time of the message delivery.

9) and 10) The SCEF entity verifies with the HSS entity whether the SCS entity is allowed to issue group messages, by the exchange of messages DIAMETER CIR and CIA.

11), 12) and 13) The SCEF entity triggers the activation of the multicast bearer with the BM-SC entity, by the exchange of the messages DIAMETER GAR and GAA.

14) The SCEF entity sends a response to the SCS entity to indicate that the group message request has been accepted.

15) The group message transfer can then take place, from the SCS entity to the SCEF entity, then from the SCEF entity to the BM-SC entity and finally from the BM-SC entity to the terminals.

10.4.3. *Event monitoring configuration*

Events of which the SCEF entity wishes to be notified are provided by either the HSS entity, the MME entity or the PGW entity.

The configuration is subject to a single process when event monitoring is for a single terminal, or to a group process when event monitoring is for multiple terminals.

In the case of a single process, the messages for event monitoring configuration at the MME level can be passed through the HSS entity or directly forwarded by the SCEF entity.

The messages for event monitoring configuration at the PGW level pass through the PCRF entity.

The event configuration procedure is also used to delete a previously configured event monitoring or to replace a previously configured event monitoring with a new event monitoring.

10.4.3.1. *HSS and MME configuration*

The procedure for configuring event monitoring at the MME and HSS level is described in Figure 10.11, for a single process.

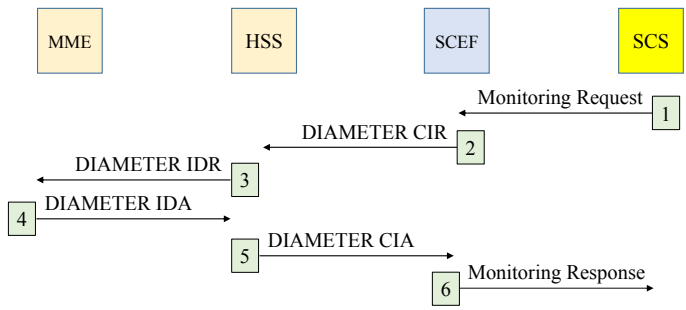

Figure 10.11. *HSS and MME configuration: single process*

1) The SCS entity sends to the SCEF entity a monitoring request by indicating the external identifier or the MSISDN, the type and the duration of monitoring.

2) The SCEF entity transfers to the HSS entity the message DIAMETER CIA containing the received information in order to configure the event monitoring on the HSS or MME entity.

3) If the event monitoring is supported by the MME entity, the HSS entity transfers the received information in the message DIAMETER IDR (Insert-Subscriber-Data-Request).

4) If the event monitoring configuration is successful, the MME entity responds to the HSS entity with the message DIAMETER IDA (Insert-Subscriber-Data-Answer). If the requested event monitoring is available at the time of sending the response, the MME entity includes the event monitoring report in the response message.

5) The HSS entity responds to the SCEF entity to inform it of the acceptance of the event monitoring request in the message DIAMETER CIR. If the requested event monitoring is available at the time of sending the response message or has been received from the MME entity, the HSS entity includes an event monitoring report in the response message.

6) The SCEF entity responds to the SCS entity to inform it of the acceptance of the event monitoring request. If the SCEF entity has received an event monitoring report, it includes it in the monitoring response message.

The procedure for configuring event monitoring at the MME and HSS level is described in Figure 10.12, for a group process.

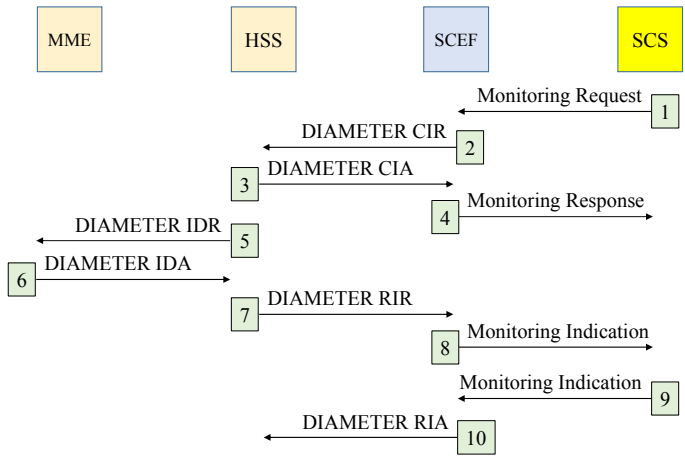

Figure 10.12. *HSS and MME configuration: group process*

1) If the SCS entity wishes to configure an event monitoring for a terminal group, it sends a monitoring request message including the group identifier and the group report hold-time.

The group report hold-time is an optional parameter to indicate that aggregated event monitoring reports detected for terminals in a group should be sent when the timer has expired.

2) and 3) When the HSS entity receives the monitoring request with a group identifier in the message DIAMETER CIR, it immediately responds to the SCEF entity with the message DIAMETER CIA indicating that the group process is in progress.

4) Upon receipt of the message DIAMETER CIA, the SCEF entity transmits the monitoring response message to the SCS entity.

5) and 6) The HSS entity sends one message DIAMETER IDR per terminal to all MME entities serving the members of the group. If the monitoring configuration succeeds, each MME entity responds to the HSS entity with the message DIAMETER IDA.

7) The HSS entity accumulates several responses for the group terminals in the hold-time of the report group. After the timer expires, it sends the responses accumulated in the message DIAMETER RIR (Reporting-Information-Request) to the SCEF entity and indicates whether the response is an intermediate message or the last group message.

8) The SCEF entity accumulates the event monitoring for the group terminals until the timer expires, and sends a monitoring indication message to the SCS entity.

9) For each received monitoring indication message, the SCS entity sends a response message to the SCEF entity.

10) The SCEF responds to the message DIAMETER RIR with the message DIAMETER RIA (Reporting-Information-Answer) indicating that monitoring indications have been received.

10.4.3.2. *PGW configuration*

The procedure for configuring event monitoring at the PGW level through the PCRF entity is described in Figure 10.13 for a single process and in Figure 10.14 for a group process.

The procedure for configuring the PGW entity is similar to that of the MME entity, for which the following changes are made:

– the messages DIAMETER CIR and CIA exchanged between the SCEF and HSS entities are replaced by the messages DIAMETER AAR (Authentication-Authorize-Request) and AAA (Authenticate-Authorize-Answer) exchanged between the SCEF and PCRF entities;

– the messages DIAMETER IDR and IDA exchanged between the HSS and MME entities are replaced by the messages DIAMETER RAR (Re-Auth-Request) and RAA (Re-Auth-Answer) exchanged between the PCRF and PGW entities;

– the messages DIAMETER RIR and RIA exchanged between the SCEF and HSS entities are replaced by the messages DIAMETER CCR (Credit-Control-Request) and CCA (Credit-Control-Answer) exchanged between the SCEF and PCRF entities.

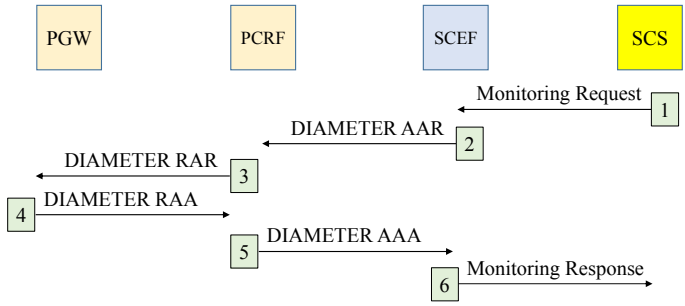

Figure 10.13. *PGW configuration: single process*

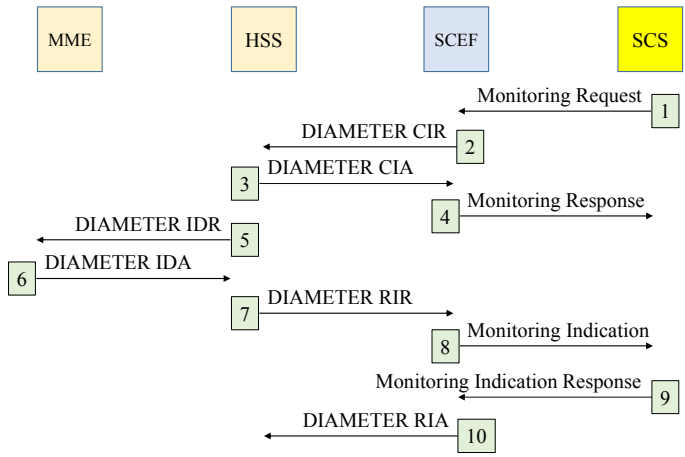

Figure 10.14. *PGW configuration: group process*

10.4.4. *NIDD transfer*

10.4.4.1. *Connection establishment*

When the terminal performs the attachment procedure to the 4G mobile network with the “non-IP” data type and the APN, the MME entity initiates a T6a connection with the SCEF entity.

The connection is initiated by the MME entity that transmits to the SCEF entity the message DIAMETER CMR (Connection-Management-Request) containing the terminal identity.

If the SCS entity has previously executed the NIDD configuration procedure with the SCEF entity, the SCEF entity responds to the MME with the message DIAMETER CMA (Connection-Management-Answer) confirming the establishment of the connection.

If the NIDD configuration procedure with the SCEF entity has not been performed, the SCEF entity may reject the connection setup request or initiate a NIDD configuration procedure with the SCS entity.

10.4.4.2. *NIDD configuration*

The NIDD configuration is associated with a single terminal or a group of terminals. The procedure can also be used to replace or delete existing configuration information.

In order to avoid any errors for uplink transmission, the NIDD configuration procedure should be performed by the SCS entity before the terminal establishes a connection on the T6a interface. The downlink non-IP data from the SCS entity may be contained in the NIDD configuration request message.

The NIDD configuration procedure is described in Figure 10.15.

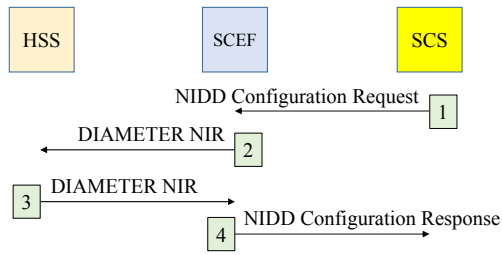

Figure 10.15. *NIDD configuration*

1) The SCS entity sends to the SCEF entity an NIDD configuration request message, which contains the terminal or the group identifier.

An optional field is used to indicate what the SCEF entity shall do if the T6a connection is not established and if data on the downlink must be sent: wait for the T6a connection to be established, reply with an error message or arm a timer.

2) The SCEF entity transmits the message DIAMETER NIR (NIDD-Information-Request) to the HSS entity to authorize the NIDD configuration request.

3) The HSS entity responds with the message DIAMETER NIA (NIDD-Information-Answer) to accept the request from the SCEF entity.

If the terminal identity uses an external identifier, the HSS entity provides the correspondence with the IMSI and/or MSISDN.

If a group identifier is included in the authorization request, the HSS entity provides the correspondence with a list of external identifiers and maps the identifiers external to the IMSI and/or MSISDN.

4) The SCEF entity sends a response message to the SCS entity to acknowledge the NIDD configuration request.

10.4.4.3. *Downlink data*

The procedure for transmitting downlink NIDD is described in Figure 10.16.

1) The SCS entity transmits downlink NIDD to the SCEF entity.

Maximum latency is an optional field used to indicate the maximum acceptable value. Zero latency indicates that buffering is not allowed. If maximum latency is not provided, the SCEF entity determines the acceptable delay based on local policies.

Other optional fields may be used: the priority of NIDD, the acknowledgment of data, the action to be taken if the T6a connection is not established and the sequence number if NIDD refers to previous data.

2) The SCEF entity verifies whether the SCS entity is allowed to send NIDD and whether or not it has exceeded the number of bytes or the bit rate. These values were transmitted by the MME entity during the T6a connection.

If the T6a connection is established, the SCEF entity sends to the MME entity the message DIAMETER TDR (MT-Data-Request) containing the NIDD and indicating the maximum duration during which the SCEF entity is ready to wait for a MME entity response and delay for the retransmission of NIDD.

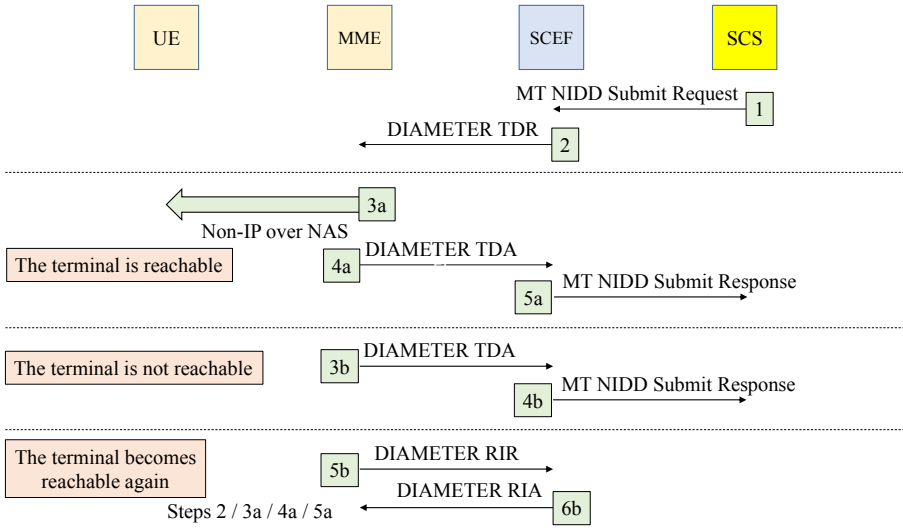

Figure 10.16. *Downlink NIDD transfer*

3a) If the terminal is in the ECM_CONNECTED state, the MME entity may issue the NIDD carried by the NAS message to the terminal.

If the terminal is idle, the MME entity initiates the paging procedure so that the terminal enters the ECM_CONNECTED state.

4a) The MME entity may receive an acknowledgment of NIDD from the terminal or eNB entity, or may not receive an acknowledgment. In these different cases, the MME entity responds to the SCEF entity with the message DIAMETER TDA (MT-Data-Answer) to acknowledge receipt of NIDD.

5a) The SCEF entity sends a response to the SCS entity indicating whether the NIDD receipt has been received or not.

3b) If the MME knows that the terminal is temporarily unreachable, it responds to the SCEF entity with the message DIAMETER TDA indicating the cause (e.g. the terminal is not reachable for energy-saving reasons). The MME entity shall notify the SCEF entity when the terminal is reachable.

If the maximum retransmission time has been included in the SCEF request, the MME entity may indicate the time at which the SCEF entity shall retransmit the data.

4b) The SCEF entity may respond to the SCS entity to inform it of the results received from the MME entity. If the SCEF entity receives from MME the cause indicating that the terminal is temporarily unreachable due to power saving, it can buffer the NIDD.

5b) and 6b) When the MME entity detects that the terminal is reachable, it informs the SCEF entity with the message DIAMETER RIR, acknowledged by the SCEF response with the message DIAMETER RIA.

The procedure continues with steps 2 (transfer of NIDD to the MME entity), 3a (transfer of NIDD to the terminal), 4a (acknowledgment of the MME entity) and 5a (acknowledgment of the SCEF entity).

10.4.4.4. *Uplink data*

The procedure for transmitting uplink NIDD is described in Figure 10.17.

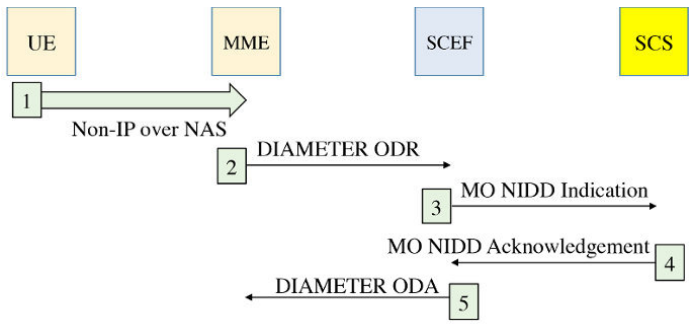

Figure 10.17. *Uplink NIDD transfer*

1) The terminal transmits the NIDD to the MME entity in a NAS message.

2) The MME entity transfers the NIDD to the SCEF entity in the message DIAMETER ODR (MO-Data-Request).

3) The SCEF entity transfers the NIDD to the SCS entity.

4) The SCS entity acknowledges the receipt of the data towards the SCEF entity.

5) The SCEF entity uses the message DIAMETER ODA (MO-Data-Answer) to inform the MME entity that the NIDD has been successfully delivered.

11

MTC Service – Radio Interfaces

11.1. Introduction

LTE (Long-Term Evolution) radio access was initially designed for high-speed communications, taking into account high mobility and low latency for data transport.

Using LTE radio access for connected objects exposes different constraints such as battery life and terminal cost, and decreases the speed and latency requirements.

The reduction of the radio channel bandwidth is one of the factors making it possible to keep the objectives fixed for the connected objects:

– the bandwidth is reduced to 1.4 MHz or 5 MHz for the LTE-M radio interface;

– the bandwidth is reduced to 180 kHz for the NB-IoT (NarrowBand Internet of Things) radio interface.

The reduction of the modulation index and the absence of a MIMO (Multiple Input Multiple Output) mechanism also contribute to reducing energy consumption and lowering terminal costs.

The power saving mode (PSM), on the one hand, and the extended discontinuous reception (eDRX), on the other hand, are complementary mechanisms that reduce the terminal power consumption during standby or when the terminal radio interface and the functions relating to radio resource control (RRC) are switched off.

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

11.2. Special features

11.2.1. *PSM feature*

The PSM feature is designed to help terminals to reduce battery consumption and potentially reach 10 years of battery life.

The PSM feature is similar to a power off, but the terminal maintains the context, which avoids turning off the terminal and reconnecting to the network when restarting.

When a device starts the PSM procedure, it provides two timers (T3324 and T3412). The switch-off time of the radio interface and the functions associated with the RRC protocol is the time difference between these two timers (Figure 11.1).

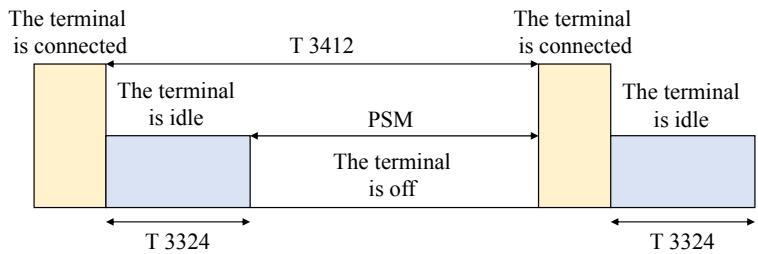

Figure 11.1. *PSM*

During the activation of timer T3324, the terminal in the idle state listens for paging. When timer T3324 expires, the terminal enters PSM until timer T3412 expires. The terminal is no longer reachable by the network but can at any time request the restoration of a session.

The network can accept these values or define others. The network then keeps the context of the terminal and the terminal remains attached. If a terminal wakes up and sends data before timer T3412 expires, no attachment procedure is necessary.

The terminal cannot be contacted by the paging procedure when it is off. The network may choose to store the incoming data for transfer to the terminal once it wakes up.

The maximum time that a terminal can be accessed for is 186 minutes (timer T3324). The maximum time that a terminal can be powered down for is approximately 413 days (timers T3412 and T3324).

11.2.2. *eDRX feature*

The extended discontinuous reception (eDRX) is an extension of an existing feature, which can be used by terminals to reduce power consumption. The eDRX configuration can be used without PSM or in combination for additional energy savings.

The eDRX feature extends the time interval during which the terminal does not listen to the network. It may be entirely acceptable that the terminal will not be reachable for the cycle duration, between 20.48 and 10 485.76 seconds for the NB-IoT radio interface and between 5.12 and 2621.44 seconds for the LTE-M radio interface.

11.2.3. *Coverage extension*

Coverage extension (CE) improves coverage by using repetition techniques for physical channels relating to the user and control planes.

Mode CE A (respectively CE B) supports up to 32 repetitions (respectively 2048 repetitions). This mode (respectively CE B) improves the maximum coupling loss (MCL) by 5 dB (respectively 15 dB).

Mode CE A is the default operating mode. The difference in coverage between a terminal Cat. M1 operating in mode CE A and a terminal Cat. 1 lies in the fact that the terminal Cat. M1 has only one receiver and a reduced transmission power. This difference is compensated for by using a small number of repetitions.

Mode CE B is an optional extension offering a greater coverage improvement at the expense of capacity and latency. It was primarily designed to provide indoor coverage. For this reason, it is intended for applications that require limited data rates or volumes.

11.3. LTE-M interface

11.3.1. *Radio channel*

The LTE-M radio interface uses the narrow bandwidth concept to assign sub-carriers of the LTE radio channel. Each narrow bandwidth comprises six consecutive physical resource blocks (PRBs).

The LTE-M interface uses the concept of wide bandwidth to allocate a higher bandwidth, consisting of four narrow bandwidths, when possible, or one to three narrow bandwidths when it is not possible.

11.3.2. *Guard time*

Although a terminal has a bandwidth of 1.4 MHz, it can access different narrow bands for each sub-frame. If the transmission involves repetition over multiple sub-frames, a frequency hopping between the sub-frames can be applied. Frequency hopping takes place between different narrow bands and in blocks of 1 to 16 sub-frames depending on the CE mode.

Two OFDM (Orthogonal Frequency-Division Multiplexing) symbols are pre-empted to form the guard time when frequency hopping occurs. Figure 11.2 describes the different scenarios for the uplink.

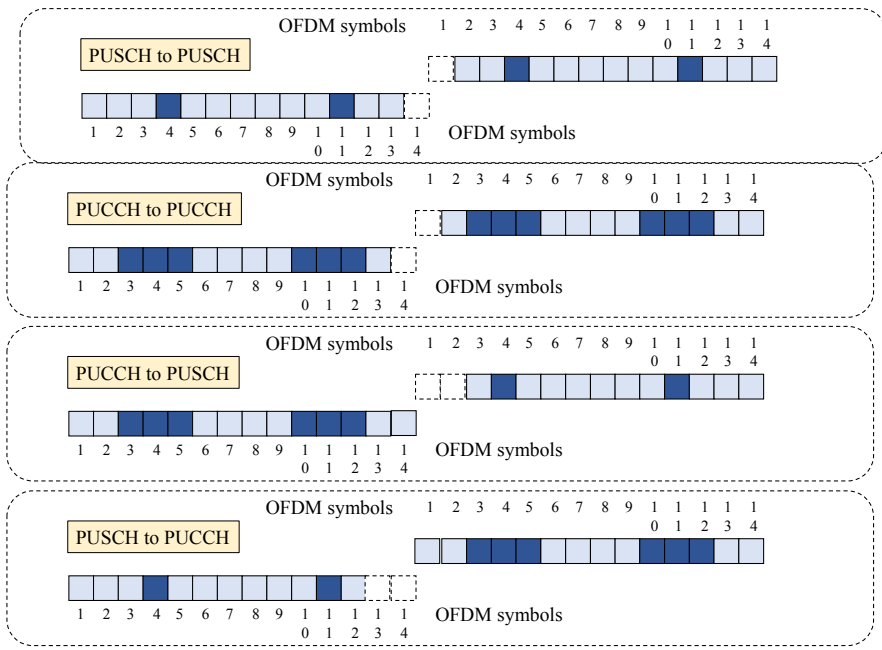

Figure 11.2. *Guard time*

When both sub-frames carry the same physical channel (PUSCH or PUCCH), each sub-frame is pre-empted with an OFDM symbol.

When both sub-frames carry different physical channels (PUCCH and PUSCH), pre-emption only takes place on the physical uplink shared channel (PUSCH).

11.3.3. *Physical channels*

11.3.3.1. *PBCH*

The LTE-M radio interface uses the same physical broadcast channel (PBCH) as the LTE radio interface, with optional repetitions.

The PBCH is divided into two parts:

– the basic physical channel, which is the channel of the LTE radio interface. This channel is transmitted in the first sub-frame of each frame with a periodicity of 40 ms;

– the physical repetition channel for which the OFDM symbols of the slot are repeated up to five times, depending on the duplex mode and the length of the cyclic prefix.

Repetitions occur in sub-frame 9 of the previous frame and in sub-frame 0 of the current frame for the frequency-division duplex (FDD) (Figure 11.3). For time-division duplex (TDD), repetitions occur in sub-frames 0 and 5 of the same radio frame.

For the FDD mode, all symbols of the basic physical channel are repeated four times if the cyclic prefix is normal and three times if the cyclic prefix is extended. For the TDD mode, if the cyclic prefix is extended, all symbols are repeated three times, and if the cyclic prefix is normal, symbols 0 and 1 are repeated five times and symbols 2 and 3 are repeated three times.

11.3.3.2. *MPDCCH*

The MTC (Mobile Type Communication) physical downlink control channel (MPDCCH) carries specific downlink control information (DCI):

– format 6-0 is used to allocate a resource to the mobile for the uplink on the PUSCH;

– format 6-1 is used to allocate a resource to the mobile for the downlink on the physical downlink shared channel (PDSCH);

– format 6-2 is used to indicate the presence of paging in the PDSCH.

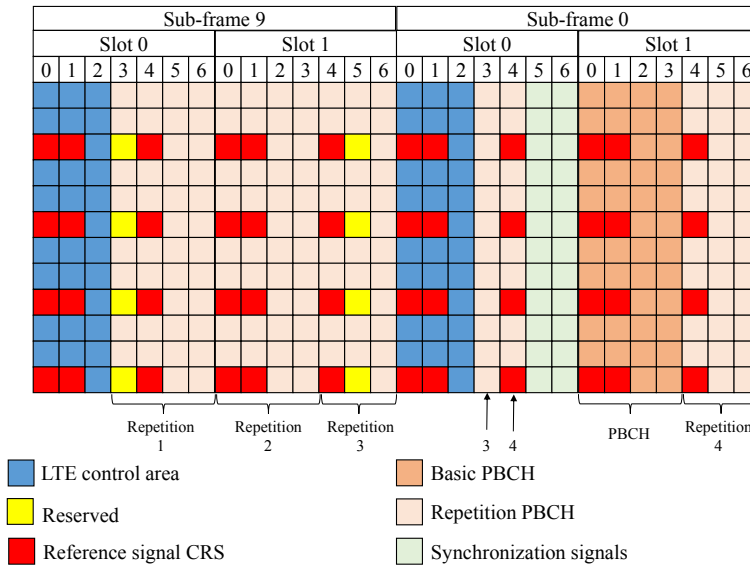

Figure 11.3. *PBCH structure*

In the case of mode CE A, the power control of the PUCCH and PUSCH is provided by formats 3 and 3A. In the case of mode CE B, the transmission power is set to the maximum value.

The processing done for the MPDCCH and ePDCCH (enhanced PDCCH) is very similar, the main differences being repetitions and frequency hopping.

The MPDCCH occupies in two, four or six PRBs transmitted in a narrow bandwidth and starts after the symbols assigned to the PDCCH.

The number of repetitions is defined by a combination of static configuration and dynamic selection for a given transmission.

11.3.3.3. *PDSCH*

The LTE-M radio interface uses the same PDSCH as the LTE radio interface, with optional repetitions and frequency hopping.

The transmission modes are mode 1 (single antenna), mode 2 (transmission diversity), mode 6 (precoding based on a closed-loop codebook) and mode 9 (precoding based on a codebook, one layer). Mode 6 is only supported for mode CE A, whereas modes 1, 2 and 9 are supported for both modes CE A and CE B.

The LTE-M radio interface does not support the MIMO mechanism because most terminals are low cost and have a single receiving antenna.

The PDSCH is transmitted in consecutive sub-frames. These sub-frames are transmitted in blocks whose number is equal to:

– 1 in mode FDD and in mode CE A;

– 4 in mode FDD and in mode CE B;

– 1 in mode TDD and in mode CE A;

– 10 in mode TDD and in mode CE B.

If the PDSCH is repeated over several sub-frames, frequency hopping between sub-frames may optionally be applied.

The number of repetitions is a combination of a static configuration (four values for mode CE A, eight values for mode CE B) and a dynamic selection of the value for a given transmission.

The system information block 1 (SIB1), transported in the PDSCH, has no fixed location in the time domain. Two narrow bandwidths are selected based on the physical-layer cell identity (PCI).

The SIB1 is transmitted with a periodicity of eight frames in the time domain. The location of the SIB1, corresponding to the frame number and the sub-frame number, depends on the number of repetitions and the value of the PCI.

11.3.3.4. *PUSCH*

The LTE-M radio interface uses the same PUSCH as the LTE radio interface, with optional repetitions and frequency hopping.

As for the PDSCH, the number of repetitions is defined by a combination of static configuration and dynamic selection for a given transmission.

11.3.3.5. *PUCCH*

As with the LTE radio interface, the physical uplink control channel (PUCCH) carries uplink control information (UCI), with a limitation of the format type, given the limitation of the transmission modes:

– format 1 supports the scheduling request (SR) for which no bit is transmitted, the evolved node base station (eNB) detecting only the presence of energy in the PUCCH;

– format 1A supports the information HARQ (Hybrid Automatic Repeat reQuest) indicator (HI) corresponding to a positive or negative acknowledgment bit of a transport block received on the PDSCH;

– format 2 supports channel state information (CSI) relating to the PDSCH, corresponding to 20 bits.

The PUCCH is transmitted in blocks of sub-frames, each block being the subject of a frequency hopping. Frequency hopping is not used if the number of repetitions is smaller than the number of sub-frames in a block.

11.3.3.6. *PRACH*

The physical random access channel (PRACH) transports the random access preamble, transmitted in six PRB resources.

The PRACH configuration is a combination of configurations indicated by the cell and parameters specific to the terminal.

11.4. NB-IoT interface

11.4.1. *Radio channel*

The NB-IoT interface occupies a frequency band of 180 kHz, which corresponds to 12 sub-carriers in the frequency domain, for example a PRB.

Three operation modes are defined (Figure 11.4):

– the autonomous operation which can be deployed in the GSM radio channel, for example, and whose bandwidth is equal to 200 kHz;

– the guard-band operation which can be deployed in the available guard band of the LTE radio channel;

– the operation in the useful bandwidth of the LTE radio channel.

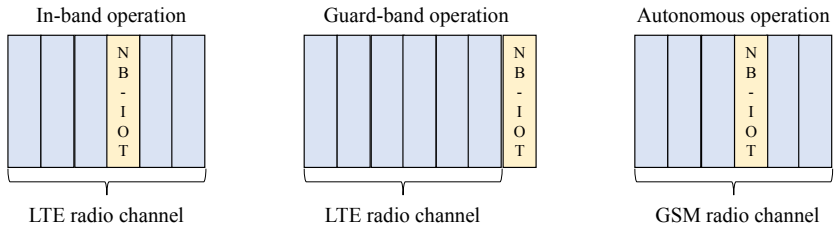

Figure 11.4. *NB-IoT radio channel*

11.4.2. *Resource block*

The PRB, for the downlink, consists of 12 sub-carriers spaced by 15 kHz, in the frequency domain.

For the uplink, the eNB entity defines the spacing between the subcarriers (Figure 11.5):

– a spacing of 15 kHz, as for the downlink;

– a spacing of 3.75 kHz. The PRB then consists of 48 subcarriers.

The slot consists of seven OFDM symbols, whose duration depends on the spacing between the sub-carriers (Figure 11.5):

– 0.5 ms in the case of a spacing of 15 kHz between the sub-carriers;

– 2 ms in the case of a spacing of 3.75 kHz between the sub-carriers.

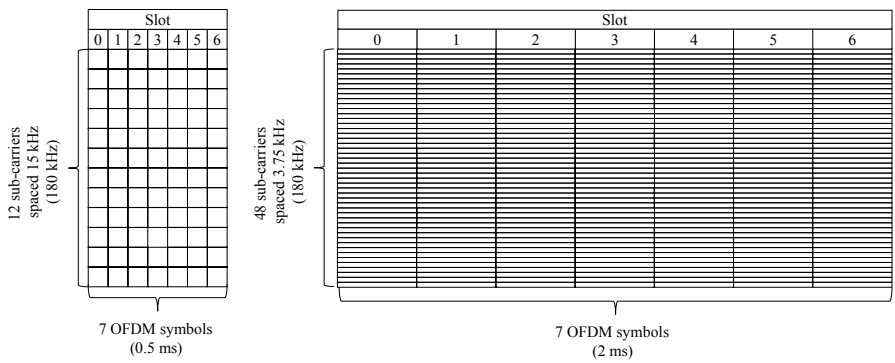

Figure 11.5. *Physical resource block*

11.4.3. *Physical signals and channels*

11.4.3.1. *NPSS and NSSS*

The narrowband primary synchronization signal (NPSS) carries a Zadoff–Chu sequence of 11 OFDM symbols. This sequence is fixed and therefore contains no information on the cell. The sequence is transmitted in the sub-frame 5 of each frame, which allows the terminal to acquire the frame synchronization (Figure 11.6).

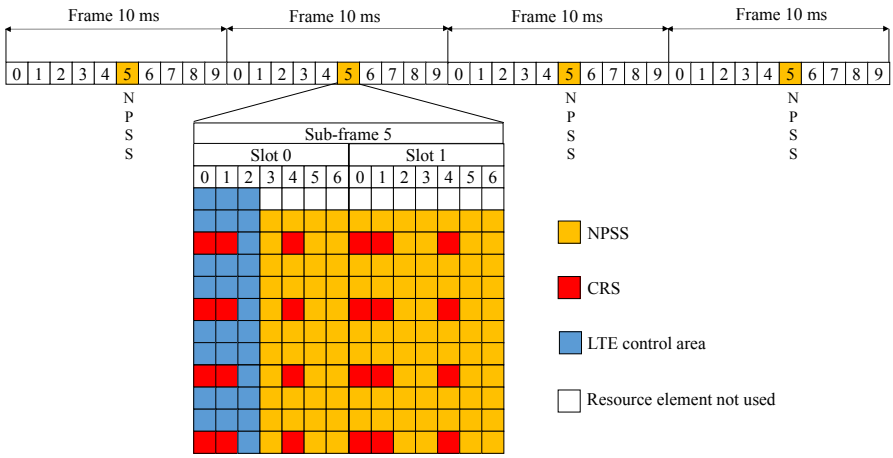

Figure 11.6. *NPSS*

The narrowband secondary synchronization signal (NSSS) has a Zadoff–Chu sequence of 131 resource elements. Four types of sequence are used with a periodicity of 80 ms. The sequence also makes it possible to deduce the PCI. As for the LTE radio interface, 504 values are defined. The sequence is transmitted in the sub-frame 9 of each even frame (Figure 11.7).

The first three OFDM symbols are omitted because they can carry the PDCCH when the NB-IoT radio interface is used in the LTE radio channel band.

When the terminal synchronizes with NPSS and NSSS, it may not know the operation mode (1, 2 or 3 OFDM symbols for the PDCCH). Therefore, this restriction applies to all operation modes.

The two synchronization signals are punctured by the cell-specific reference signal (CRS), assuming the use of four antenna ports.

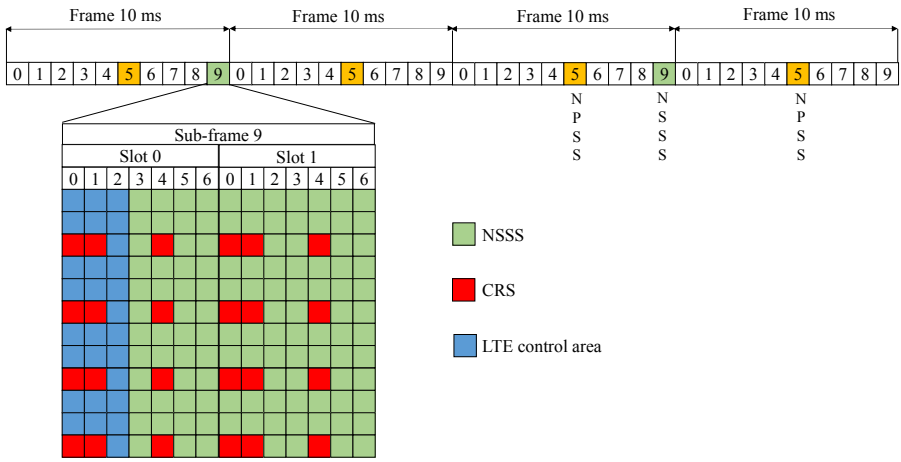

Figure 11.7. *NSSS*

The PRB numbers of the LTE radio interface assigned to the NB-IoT radio interface for synchronization are provided in Table 11.1, in the case of operation in the LTE radio channel.

Bandwidth	PRB number
3 MHz	2, 12
5 MHz	2, 7, 17, 22
10 MHz	4, 9, 14, 19, 30, 35, 40, 45
15 MHz	2, 7, 12, 17, 22, 27, 32, 42, 47, 52, 57, 62, 67, 72
20 MHz	4, 9, 14, 19, 24, 29, 34, 39, 44, 55, 60, 65, 70, 75, 80, 85, 90, 95

Table 11.1. *PRBs allocated to the synchronization signals*

11.4.3.2. *NRS*

The narrowband reference signal (NRS) is transmitted in each sub-frame for one or two antenna ports. Its location is determined from the PCI parameter. When the NRS is transmitted on two antenna ports, the resource elements assigned to the antenna port 1 are set to zero in the resource blocks corresponding to the antenna port 0, and vice versa (Figure 11.8).

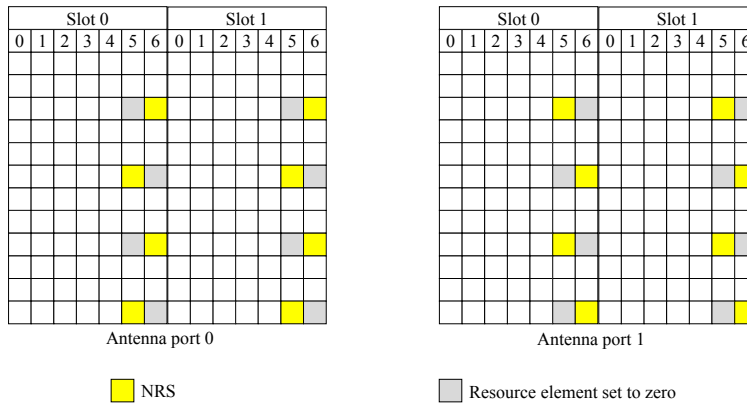

Figure 11.8. *NRS*

11.4.3.3. *NPBCH*

The narrowband PBCH (NPBCH) carries the master information block narrowband (MIB-NB) which contains the following information:

– the data for the partial calculation of the frame and hyper-frame numbers;

– the scheduling of the SIB1-NB;

– the operating mode of the NB-IoT radio interface.

The NPBCH is transmitted in sub-frame 0 and distributed over eight blocks. The first block is repeated on eight consecutive sub-frames 0. The same operation is performed on the next seven blocks. Each block is transmitted over a period of 80 ms and the periodicity of the MIB-NB is 640 ms (Figure 11.9).

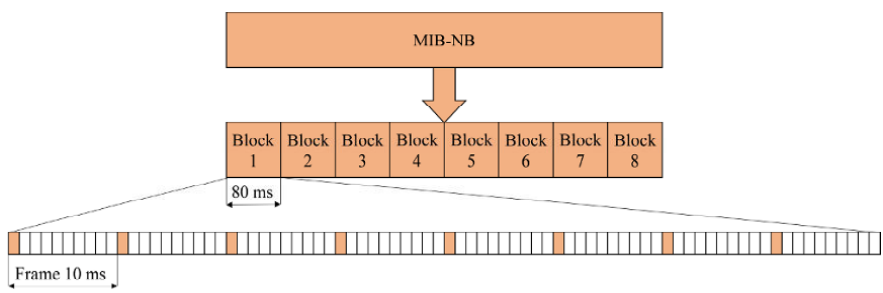

Figure 11.9. *NPBCH: repetition structure*

As for the NPSS and NSSS, the first three OFDM symbols are omitted and the NPBCH is punctured by the CRS. The NPBCH is also punctured by the NRS, for which it is assumed that two antenna ports are used (Figure 11.10).

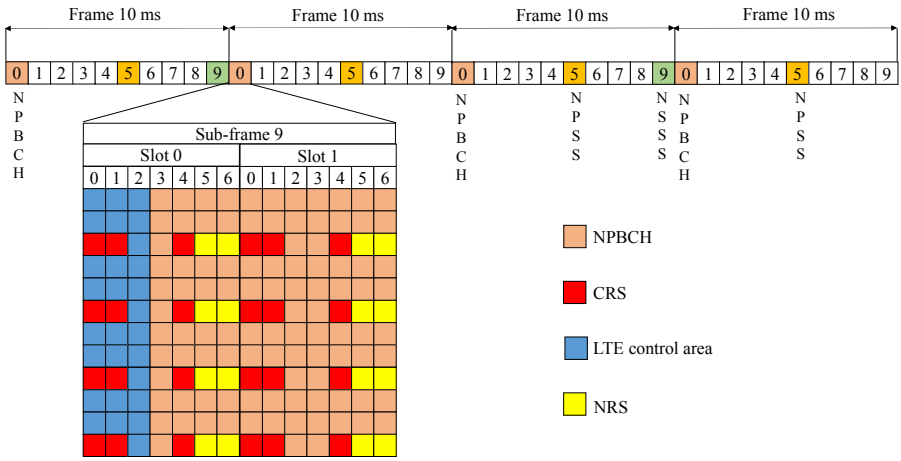

Figure 11.10. *NPBCH: sub-frame structure*

The PRB numbers of the LTE radio interface assigned to the NB-IoT radio interface for the NPBCH are provided in Table 11.1.

11.4.3.4. *NPDCCH*

The narrowband PDCCH (NPDCCH) carries the DCI, for which three formats are defined:

– format N0: the DCI indicates the resources that the terminal must use for uplink data transmission;

– format N1: the DCI defines the location of the terminal data in the NPDSCH and the repetition frequency;

– format N3: the DCI provides additional information, such as paging or changing system information.

For operation in the bandwidth of the LTE radio channel, the NPDCCH is punctured by the NRS and CRS. To avoid conflict with LTE radio control channels, the PDCCH start-up symbol is indicated by the SIB1-NB (Figure 11.11).

For each sub-frame, two narrowband control channel elements (NCCE) are defined, NCCE0 and NCCE1. Two formats are defined to use them:

– format 0 occupies one NCCE;

– format 1 occupies both NCCE.

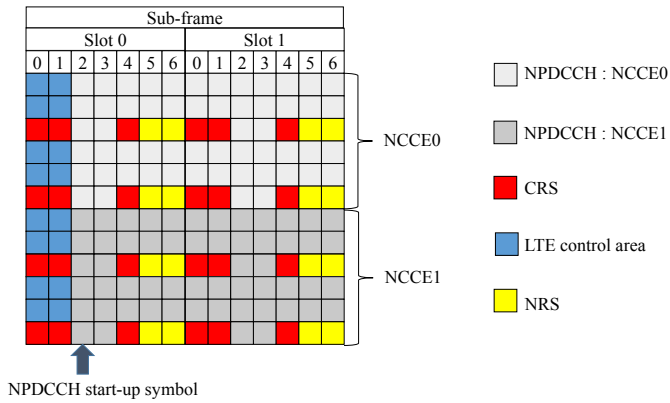

Figure 11.11. *NPDCCH*

For a standalone or guard-band operation, the NPDCCH is only punctured by the NRS. The size of the reserved area for the control channels of the LTE radio interface is void.

In order for the terminal to find the control information with reasonable decoding complexity, the NPDCCH defines the following search spaces:

– type 1: the common search space for paging;

– type 2: the common search space for random access;

– the search space dedicated to the terminal.

The location of the NPDCCH for the type-1 search space is determined from the candidate sub-frames.

The parameters for calculating the location of the NPDCCH for the type-2 search space are provided in the SIB2-NB.

The parameters for calculating the location of the NPDCCH for the dedicated search space are provided in the message RRC *ConnectionSetup*.

The NPDCCH can operate in the bands used for mobile synchronization, defined in Table 11.1, or in dedicated bands.

11.4.3.5. *NPDSCH*

The narrowband PDSCH (NPDSCH) carries, on the one hand, the different RRC messages corresponding to the SIB-NB, paging, common messages and dedicated messages, and, on the other hand, the terminal traffic (IP packets or non-IP packets).

The NB-IoT interface supports, for the downlink, a transmission on two antenna ports, for SFBC (Space Frequency Block Coding) diversity.

Dedicated messages may encapsulate NAS (Non-Access Stratum) messages exchanged between the terminal and the mobility management entity (MME). NAS messages can carry terminal traffic.

For the different RRC messages, with the exception of the system information, and for the terminal traffic, the sub-frame structure assigned to the NPDSCH has the same characteristics as the NPDCCH.

The SIB1-NB provides the following information:

– cell access information (country code, operator code, location code, cell identity);

– information relating to the selection of the cell (minimum level of reception);

– information relating to the scheduling of other SIB-NB.

The SIB1-NB is transmitted with a periodicity of 256 frames and a repetition of 4, 8 or 16 times. The size of the transport block and the number of repetitions are indicated in the MIB-NB.

The SIB1-NB is transmitted in the sub-frame 4. The frame on which the SIB1-NB system information starts is determined by the number of repetitions and the PCI parameter.

11.4.3.6. *NPUSCH*

Two formats are defined on the narrowband PUSCH (NPUSCH):

– format 1 relates to transport channel data with transport blocks not exceeding 1000 bits;

– format 2 contains UCI which are limited to an acknowledgment (HARQ) of the data received on the NPDSCH.

The resource unit (RU) is the smallest unit for mapping a transport block. Its structure depends on the format and spacing of the sub-carriers:

– for the sub-carrier spacing of 3.75 kHz and for format 1, the resource unit consists of a sub-carrier in the frequency domain and 16 slots in the time domain;

– for the sub-carrier spacing of 15 kHz and for format 1, there are four options listed in Table 11.2;

– for format 2 and for the sub-carrier spacing of 3.75 kHz or 15 kHz, the resource unit consists of a sub-carrier and four time slots.

Sub-carrier number	Slot number
1	16
3	8
6	4
12	2

Table 11.2. *RU structure*

11.4.3.7. *DMRS*

The demodulation reference signal (DMRS) is multiplexed with the NPUSCH. The resource elements assigned to the DMRS depend on the format and spacing between the sub-carriers (Figure 11.12).

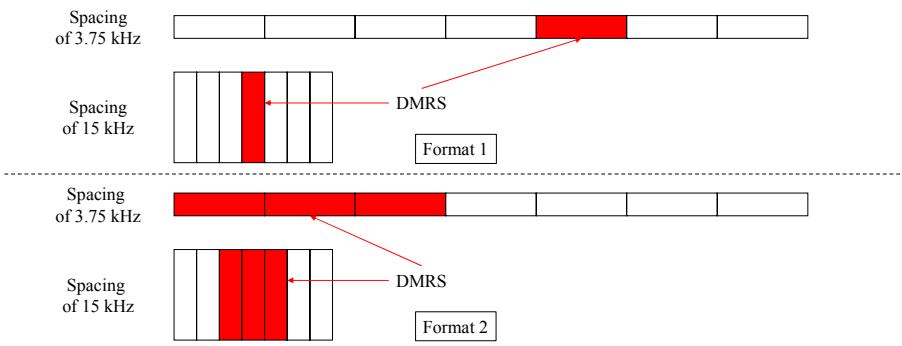

Figure 11.12. *DMRS*

11.4.3.8. *NPRACH*

The preamble, transmitted on the Narrowband PRACH (NPRACH), is based on symbol groups on a single sub-carrier. Each symbol group has a cyclic prefix followed by five symbols (Figure 11.13).

Two preamble formats are defined, format 0 and format 1, which differ in length. The five symbols have a duration of T_{SEQ} = 1.333 ms, with a cyclic prefix of T_{CP} = 67 µs for format 0 and 267 µs for format 1, and a total length of 1.4 ms and 1.6 ms, respectively (Figure 11.13). The preamble format to be used is broadcasted in the SIB2-NB system information.

The preamble is composed of four groups of consecutive symbols. Frequency hopping is applied for each group of symbols, transmitted on a different subcarrier. The repetition number, 1, 2, 4, 8, 16, 32, 64 or 128 times, is indicated by the SIB2-NB. The same transmission power is used at each repetition.

The resources of the NPRACH are produced with periodicities between 40 ms and 2.56 s. The beginning of the period is provided in the SIB2-NB. The number of repetitions and the format of the preamble determine the end of each period.

In the frequency domain, a sub-carrier spacing of 3.75 kHz is applied. The NPRACH resources occupy a contiguous set of 12, 24, 36 or 48 subcarriers (Figure 11.13).

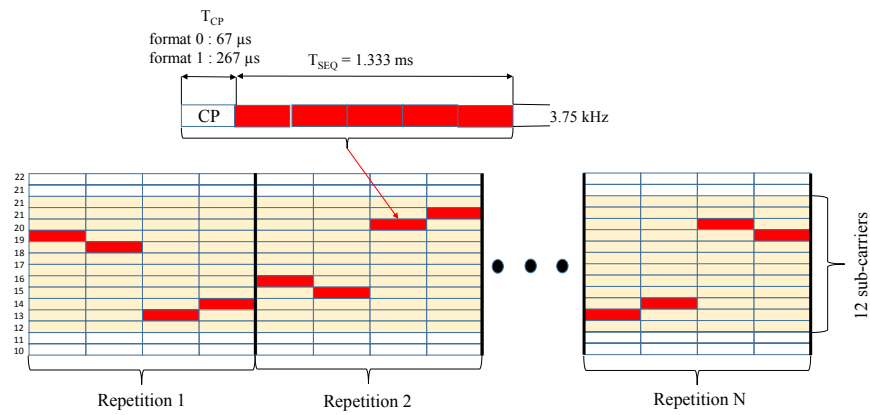

Figure 11.13. *NPRACH*

12

MBB Service – 5G Integration

12.1. Deployment options

Like in previous generations, the 3GPP standard organization defines a 5G core network (5GC) and a 5G radio access network (5G NR).

Unlike previous generations which simultaneously deployed the core network and the radio access network, the fifth generation allows the integration of fourth generation (4G) elements in different configurations:

– standalone (SA) configuration: the connection of the radio access network to the core network is set up for the user plane and the control plane;

– non-standalone (NSA) configuration: the connection of the radio access network to the core network is set up only for the user plane.

Option 2 corresponds to an SA configuration, for which the 5G NR connects to the 5GC.

Option 5 corresponds to an SA configuration, for which the evolved universal terrestrial radio access network (E-UTRAN) connects to the 5GC.

The NSA configuration implements the dual connectivity (DC) architecture, which has the following characteristics:

– the master radio access network connects to the core network for the control plane and the user plane;

For color versions of the figures in this chapter, see www.iste.co.uk/launay/lte.zip.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

– the secondary radio access network connects to the core network only for the user plane;

– the master radio access network controls the secondary radio access network.

Option 3 corresponds to the NSA configuration EN-DC (E-UTRA-NR DC) for which the E-UTRAN is the master radio access network and the 5G NR is the secondary radio access network. The connection is done on the evolved packet core (EPC).

Option 4 corresponds to the NSA configuration NE-DC (NR-E-UTRA DC) for which the 5G NR is the master radio access network and the E-UTRAN is the secondary radio access network. The connection is done on the 5GC.

Option 7 corresponds to the NSA configuration NGEN-DC (NG-RAN E-UTRA-NR DC) for which the E-UTRAN is the master radio access network and the 5G NR is the secondary radio access network. The connection is done on the 5GC.

Figure 12.1 describes the five deployment options that implement both types of configurations.

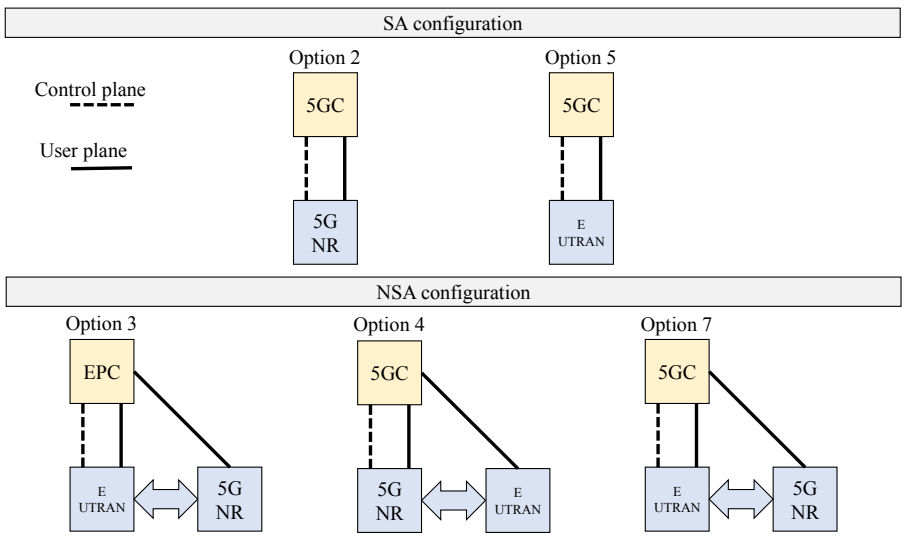

Figure 12.1. *SA and NSA configurations*

There are several ways to start the deployment of the 5G network. The main advantage of option 3 is that it only requires the deployment of the 5G NR.

Since the 5G NR will increase the existing capacity of the E-UTRAN, option 3 allows for flexible deployment when this capacity increase is needed.

More specifically, the possibility of deploying the 5G NR offers the possibility of using the spectrum above 6 GHz, whose wide frequency bands make it possible to deliver large data rates.

12.2. Functional architecture

The 5G NR consists of a single type of entity, the en-gNB (E-UTRA-NR DC next generation Node B) station (Figure 12.2).

For the control plane, the en-gNB entity connects to the evolved node base station (eNB) via the X2-C interface.

For the user plane, the en-gNB entity can connect to the core network via the S1-U interface or to the eNB entity via the X2-U interface:

– for option 3, the eNB entity connects to the core network via the S1-U interface, and the en-gNB entity connects to the eNB entity via the X2-U interface;

– for option 3a, the eNB and en-gNB entities connect to the core network via the S1-U interface;

– for option 3x, the en-gNB entity connects to the backbone via the S1-U interface, and the eNB entity connects to the en-gNB entity via the X2-U interface.

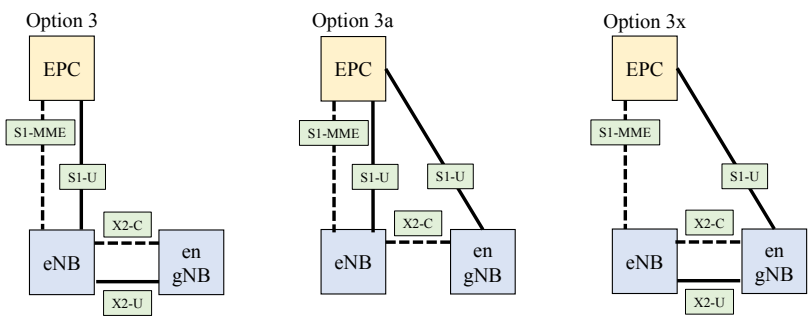

Figure 12.2. *Functional architecture*

The en-gNB entity is divided into two types of modules (Figure 12.3):

– a centralized unit (en-gNB-CU);

– one or more distributed units (en-gNB-DU).

The en-gNB-CU is connected to the eNB entity via the X2-C and X2-U interfaces and to the EPC via the S1-U interface.

Each en-gNB-DU is connected to the en-gNB-CU via the F1 interface, including the F1-C interface for the control plane and the F1-U interface for the user plane.

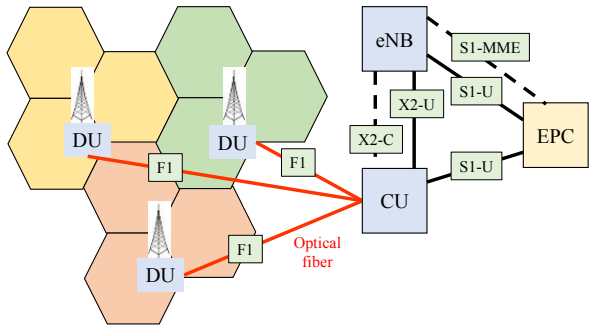

Figure 12.3. *en-gNB architecture*

12.3. Protocol architecture

12.3.1. *Radio interface*

The protocol architecture of the new radio (NR) interface has similarities to the LTE (Long-Term Evolution) radio interface described in Figure 1.4 of Chapter 1. This interface supports RRC (Radio Resource Control) signaling transmitted in the signaling radio bearer (SRB) and IP (Internet Protocol) packets transmitted in the data radio bearer (DRB) (Figure 12.4).

The NR interface introduces a new service data adaptation protocol (SDAP) that encapsulates IP packets. This protocol contains the QoS flow identifier (QFI), which indicates the level of quality of service applied to the flow.

For the LTE interface, the physical control format indicator channel (PCFICH) contains the number of OFDM (Orthogonal Frequency-Division Multiplexing) symbols used for the physical downlink control channel (PDCCH).

For the NR interface, this physical channel is deleted, the indication of the size of the PDCCH being provided by an RRC message.

For the LTE interface, the physical HARQ indicator channel (PHICH) contains the indication of a positive or negative acknowledgment (ACK/NACK) of the signal received in the physical uplink shared channel (PUSCH).

For the NR interface, this physical channel is deleted, the ACK/NACK being provided either semi-statically in an RRC message or dynamically in the downlink control information (DCI) carried in the PDCCH.

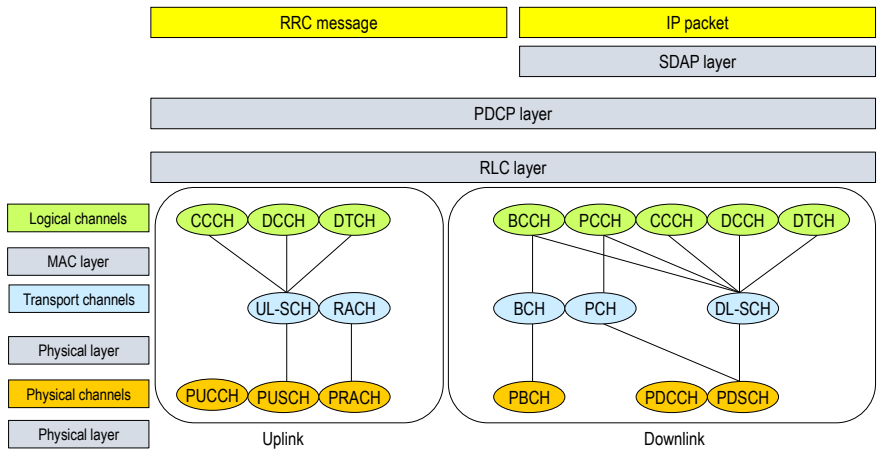

Figure 12.4. *Protocol architecture of the NR interface*

12.3.1.1. *Control plane*

The RRC protocol exists independently at the level of the two entities, the eNB master station with the 4G RRC protocol and the en-gNB secondary station with the 5G RRC 5G. An RRC connection is established independently between the mobile and the master and secondary stations.

When establishing the initial connection, the SRB1 of the eNB entity uses the 4G packet data convergence protocol (PDCP).

After establishing the initial connection, SRB1 and SRB2 may be configured to use either the 4G or 5G PDCP.

5G RRC messages generated by the en-gNB entity can then be transmitted via the eNB entity. During the initial configuration, the eNB entity sends the 5G RRC message of the en-gNB entity via SRB1 using the 5G PDCP. The following reconfigurations can be transmitted via the entity eNB or directly to the mobile via SRB3 on the NR interface.

The shared SRB is supported, which allows the duplication of 4G RRC messages generated by the master station, via the LTE-Uu interface and via the secondary station. The shared SRB support uses the 5G PDCP.

12.3.1.2. *User plane*

There are three types of DRB, corresponding to the master cell group (MCG), the secondary cell group (SCG) and the split bearer:

– MCG bearers are transmitted on the LTE interface;

– SCG bearers are transmitted on the NR interface;

– split bearers are transmitted on both the LTE and NR interfaces.

From the mobile point of view, the bearers use the following protocols (see Figure 12.5):

– 4G or 5G PDCP, 4G RLC and 4G MAC for MCG bearers;

– 5G PDCP, 5G RLC and 5G MAC for SCG bearers;

– 5G PDCP, 4G RLC and 4G MAC or 5G PDCP, 5G RLC and 5G MAC for split bearers.

From the point of view of eNB and en-gNB entities, each bearer type, MCG, SCG or split bearers, can be terminated at either the eNB entity or the en-gNB entity (Figure 12.6).

MCG bearers use 4G or 5G PDCP. Other bearers consistently use 5G PDCP.

MCG bearers use 4G RLC. SCG bearers use 5G RLC. Split bearers use 4G and 5G RLC.

MCG bearers use 4G MAC. SCG bearers use the 5G MAC 5G protocol. Split bearers use 4G and 5G MAC.

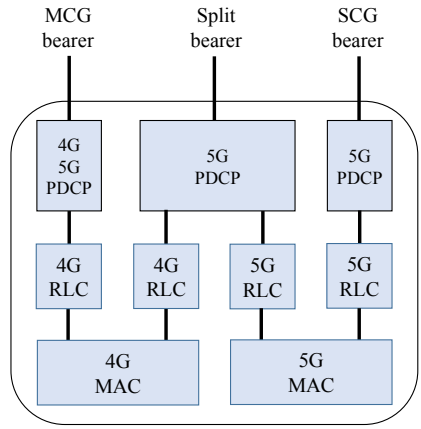

Figure 12.5. *Protocol architecture: mobile side*

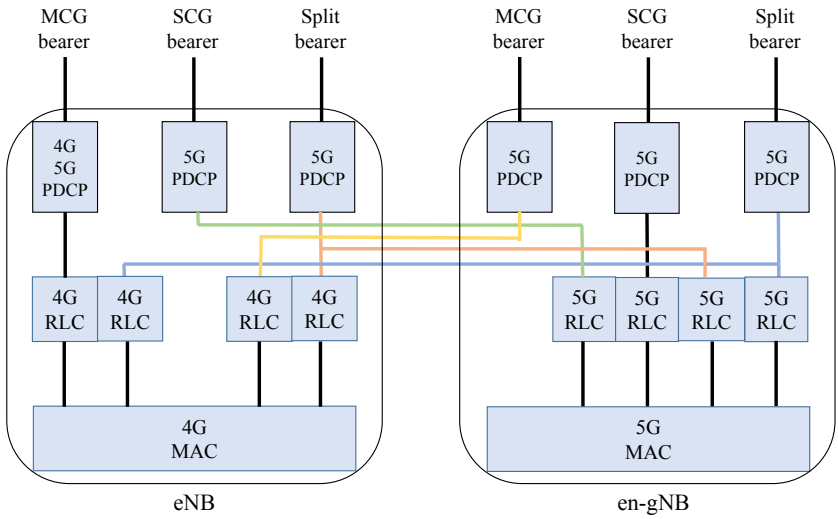

Figure 12.6. *Protocol architecture: eNB and en-gNB side*

12.3.2. *F1 interface*

Several options define the functional split between the en-gNB-CU and en-gNB-DU modules (Figure 12.7). The two main criteria that determine the choice of option are interface throughput and latency.

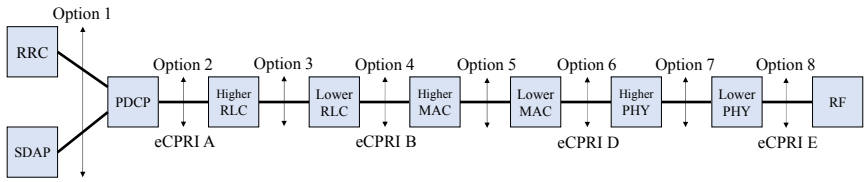

Figure 12.7. *Split configuration of the functions between CU and DU*

For option 1, the RRC and SDAP layers are hosted in the en-gNB-CU while the PDCP, RLC (Radio Link Control) and MAC (Medium Access Control) layers, as well as the physical layer (PHY) and the RF (Radio Frequency) module, are located in the en-gNB-DU.

Option 2 has similarities with the X2 interface for the user plane, and differences for the control plane since new procedures may be required.

For option 3, the split of the RLC layer is based on either the ARQ function or the direction of transmission:

– option 3.1: the lower part contains the segmentation functions, while the higher part contains the ARQ function as well as other functions of the RLC layer;

– option 3.2: the lower part is composed of the transmission functions, while the reception functions are assigned to the higher part.

For option 4, the RLC and higher layers are located in the en-gNB-CU while the MAC layer as well as the physical layer and the RF module are hosted in the en-gNB-DU.

For option 5, the higher MAC sub-layer hosted in the en-gNB-CU includes centralized scheduling and is responsible for controlling several lower MAC sub-layers, while the lower MAC sub-layer hosted in the en-gNB-DU includes functions with delay requirements such as the HARQ mechanism or random access control.

For option 6, the MAC and higher layers are hosted in the en-gNB-CU, while the physical layer and the RF module are hosted in the en-gNB-DU. The F1 interface must convey the configuration functions of the physical layer, defined by the MAC layer.

Several split configurations of the physical layer are defined. The description of the physical layer is given in Chapter 1, in Figure 1.5 for the downstream, and in Figure 1.6 for the upstream.

For option 7.1, the lower part hosted in the en-gNB-DU includes the inverse fast Fourier transform (IFFT) for both downlink and uplink, while the higher part hosted in the en-gNB-CU contains other functions.

For option 7.2, the lower part hosted in the en-gNB-DU adds the mapping function to the resource elements for both downlink and uplink.

For option 7.3, the en-gNB-CU hosts, only for the downstream, the error detection and correction code as well as the rate adaptation.

Option 8 separates the physical layer and the RF module. This split makes it possible to centralize all the processes in the en-gNB-CU entity.

In addition, the enhanced common public radio interface (eCPRI) is the subject of industrial cooperation aimed at defining the specifications available for the interface between the CU and DU modules of a radio station.

Figure 12.7 provides the correspondence between the options of the F1 interface and CPRI. Options 7.2 and 7.3 of the F1 interface also have their concordance with CPRI.

12.4. Procedures

12.4.1. *Adding a secondary node*

The procedure for adding a secondary node (en-gNB entity) is initialized by the eNB entity (master node). It is used to establish a context at the en-gNB entity to provide radio resources to the mobile.

For SCG bearers requiring radio resources, this procedure adds at least the first primary cell (PCell) (Figure 12.8).

1) The eNB entity sends to the en-gNB entity the message X2-AP SgNB Addition Request in order to allocate radio resources for the establishment of an S1-U bearer with the serving gateway (SGW).

2) If the request is accepted, the en-gNB entity determines the primary cell and possibly the secondary cells (SCell) and provides the new radio resource configuration to the eNB entity in an NR RRC configuration contained in the message X2-AP SgNB Addition Request Acknowledge.

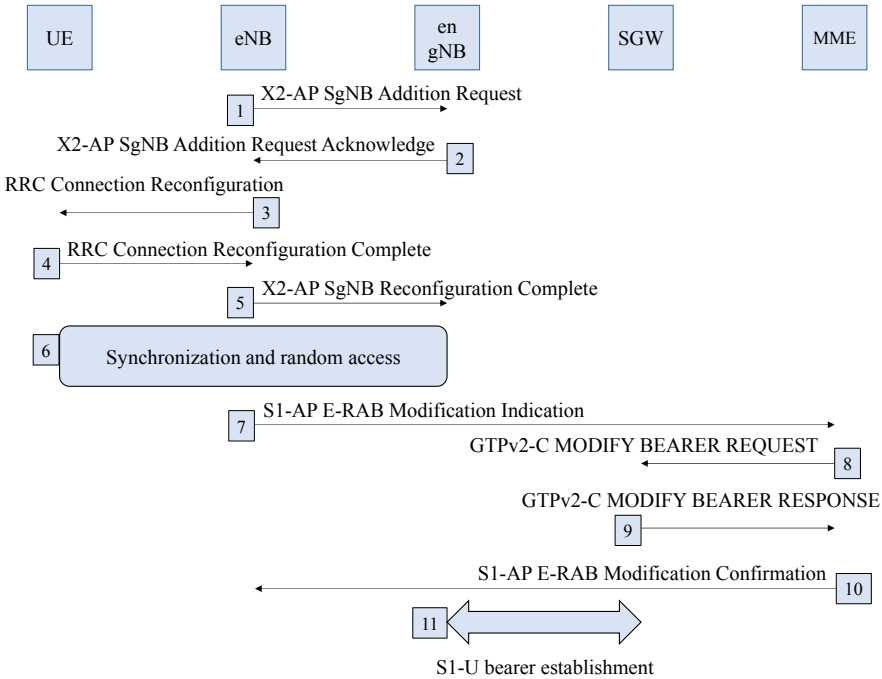

Figure 12.8. *Adding a secondary node*

3) The eNB entity transmits to the mobile the message RRC *ConnectionReconfiguration* including an NR RRC configuration message.

4) The mobile applies the new configuration and responds to the eNB entity with the message RRC *ConnectionReconfigurationComplete*, including, if necessary, an NR RRC response message.

5) The eNB entity informs the en-gNB entity of whether the mobile has successfully completed the reconfiguration procedure or not, via the message X2-AP SgNB Reconfiguration Complete, including an NR RRC response message, if it has been received from the mobile.

6) The mobile synchronizes on the PCell of the en-gNB entity and performs the random access procedure.

7) In the case of DC option 3a, to establish the SI-U bearer between en-gNB and SGW entities, the eNB entity transmits the message S1-AP E-RAB Modification Indication message to the mobility management entity (MME).

8) and 9) The establishment of the SI-U bearer continues with the exchange of GTPv2-C messages between the MME and SGW entities.

10) The MME entity acknowledges the request of the eNB entity by sending the message S1-AP E-RAB Change Confirmation.

11) The S1-U bearer between the SGW and en-gNB entities is established.

12.4.2. *Changing a secondary node*

The procedure for changing a secondary node is initialized either by the eNB entity (Figure 12.9) or by the source en-gNB entity. It is used to transfer the mobile context of the source en-gNB entity to the target en-gNB entity.

1) and 2) The procedure for changing the source en-gNB entity starts with exchanges of the messages X2-AP SgNB Addition Request and SgNB Addition Request Acknowledge between the eNB and the target en-gNB entities.

3) and 4) If the resource allocation from the target en-gNB entity has been successful, the eNB entity triggers the resource release to the source en-gNB entity with the exchange of the messages X2-AP SgNB Release Request and SgNB Release Request Acknowledge.

5) and 6) The eNB entity triggers the new configuration at the mobile level in the message RRC *ConnectionReconfiguration*, containing an NR RRC configuration message generated by the target en-gNB entity. The mobile applies the new configuration and sends the message RRC *ConnectionReconfigurationComplete*.

7) The eNB entity informs the target en-gNB entity via the message X2-AP SgNB Reconfiguration Complete that the reconfiguration procedure is successful.

8) The mobile synchronizes on the PCell of the target en-gNB entity and performs the random access procedure.

9) and 10) If the bearer uses the RLC with the acknowledgment mode, the source en-gNB entity sends the PDCP sequence number in the message X2-AP SN Status Transfer, which the eNB entity transfers to the target en-gNB entity.

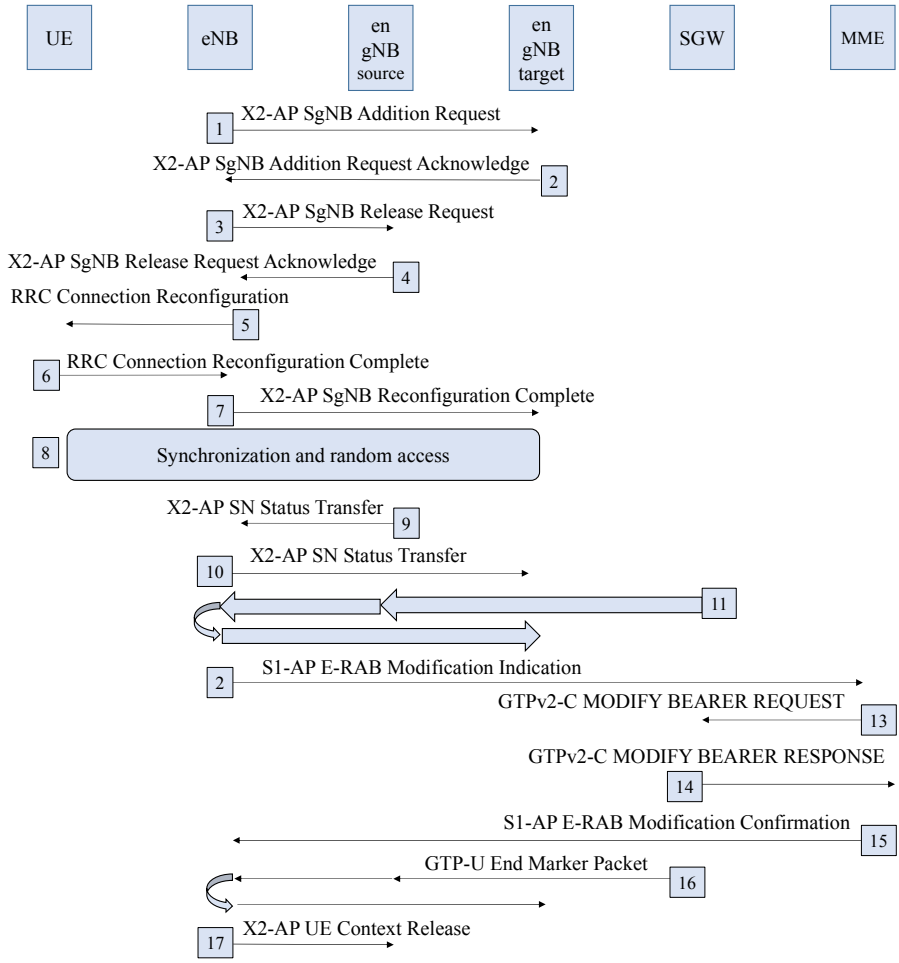

Figure 12.9. *Changing a secondary node initiated by the eNB entity*

11) If applicable, the data transfer for the downstream takes place between the en-gNB and SGW entities. It can be initialized as soon as the source en-gNB entity receives the message X2-AP SgNB Release Request from the eNB entity.

12) In the case of DC option 3a, to start the establishment of the S1-U bearer between the target en-gNB and SGW entities, the eNB entity transmits the message S1-AP E-RAB Modification Indication to the MME entity.

13) and 14) The S1-U bearer establishment continues by the exchange of GTPv2-C messages between the MME and SGW entities.

15) The MME entity acknowledges the request of the eNB entity by sending the message S1-AP E-RAB Change Confirmation.

16) The SGW entity uses the control message GTP-U End Marker Packet to notify the target en-gNB entity that traffic for the downstream will be forwarded directly.

17) Upon receipt of the message X2-AP UE Context Release, the source en-gNB entity may release the resources allocated to the mobile.

12.4.3. *Removing a secondary node*

The procedure for removing a secondary node is initialized either by the eNB entity (Figure 12.10) or by the en-gNB entity. It is used to remove the mobile context at the en-gNB entity.

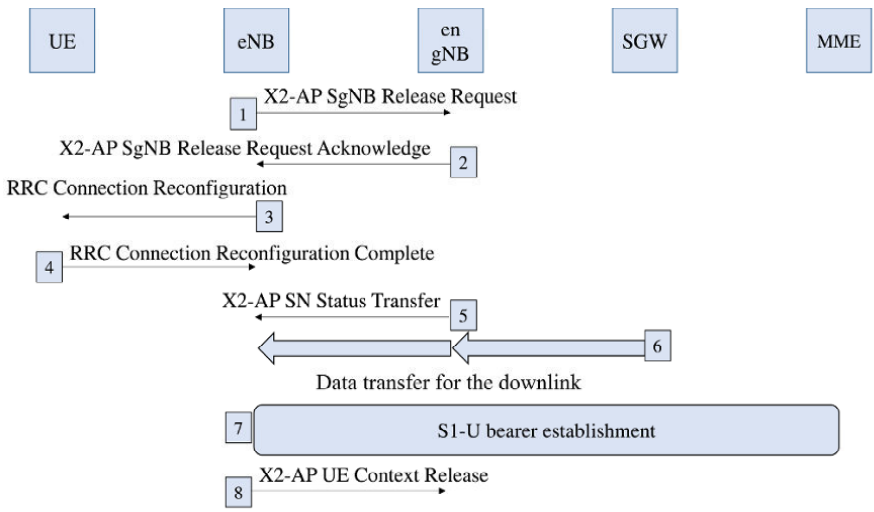

Figure 12.10. *Removing a secondary node initiated by the eNB entity*

1) The eNB entity initiates the procedure for removing the secondary node by sending to the en-gNB entity the message X2-AP SgNB Release Request. Data transfer to the eNB entity may be requested.

2) The en-gNB entity confirms the receipt by sending the message X2-AP SgNB Release Request Acknowledge.

3) and 4) In the message RRC *ConnectionReconfiguration*, the eNB entity indicates to the mobile that it must release the entire SCG bearer configuration. The mobile acknowledges the received message in the response message RRC *ConnectionReconfigurationComplete*.

5) In the case of data transfer, if the released bearer uses the acknowledgment mode for RLC, the en-gNB entity sends the message X2-AP SN Status Transfer.

6) The downlink data transfer to the eNB entity is made via the en-gNB entity.

7) In the case of DC option 3a, the S1-U bearer establishment procedure between the eNB and SGW entities takes place.

8) Upon receipt of the message X2-AP UE Context Release, the en-gNB entity may release the resources allocated to the mobile.

12.5. Transmission chain

The transmission chain of the NR interface has an identical structure to that of the LTE interface, described in Chapter 1, in Figure 1.5 for the downlink and in Figure 1.6 for the uplink.

The following sections describe the major differences in the technical characteristics of LTE and NR interfaces.

12.5.1. *Frequency bands*

Two frequency ranges (FR) are defined:

– the frequency range FR1 covers the frequency bands between 450 MHz and 6 GHz. The radio channel bandwidth is between 5 and 100 MHz;

– the frequency range FR2 covers the frequency bands between 24.250 GHz and 52.600 GHz. The radio channel bandwidth is between 50 and 400 MHz.

Several transmission modes are supported for the frequency range FR1:

– frequency-division duplex (FDD): uplink and downlink use a specific frequency band;

– time-division duplex (TDD): uplink and downlink temporally share the same frequency band;

– supplementary uplink (SUL): an additional frequency band is allocated only for uplink;

– supplementary downlink (SDL): an additional frequency band is allocated only for downlink.

The frequency range FR2 only supports the TDD mode.

The bandwidth of receiving and transmitting a mobile should not necessarily be as wide as the radio channel bandwidth and can be adjusted.

For initial access and until the mobile configuration is received, the mobile uses a bandwidth part (BWP) of the radio channel. The mobile can be configured with multiple bandwidth portions, only one of which can be active for a radio channel.

12.5.2. *Waveform*

The OFDM (Orthogonal Frequency-Division Multiplexing) signal using the cyclic prefix is the downlink waveform. The DFT-S-OFDM (Discrete Fourier Transform Spread OFDM) signal using a cyclic prefix is the uplink waveform, but the DFT-S precoding function can be disabled.

For the LTE interface, the spacing between the sub-carriers has a single value equal to 15 kHz. For the NR interface, the spacing between the sub-carriers Δf takes several values according to the parameter μ (Table 12.1):

$\Delta f = 2^{\mu} \times 15$ [kHz], with

$\mu = \{0, 1, 3, 4\}$ for the primary synchronization signal (PSS) and the secondary synchronization signal (SSS), as well as for the physical broadcast channel (PBCH);

$\mu = \{0, 1, 2, 3\}$ for the physical downlink shared channel (PDSCH), the PUSCH, the PDCCH and the physical uplink control channel (PUCCH).

The spacing between the sub-carriers is correlated with the frequency range (Table 12.1):

$\mu = \{0, 1\}$: these values are reserved for the frequency range FR1;

$\mu = \{2\}$: this value is used for the frequency ranges FR1 and FR2;

$\mu = \{3, 4\}$: these values are reserved for the frequency range FR2.

The normal cyclic prefix is supported for all spacing values between sub-carriers. The extended cyclic prefix is supported only for the value of $\mu = 2$ (Table 12.1).

μ	Spacing between sub-carriers	Cyclic prefix	PDSCH, PUSCH PDCCH, PUCCH	PSS, SSS PBCH
0	15	Normal	yes (FR1)	yes (FR1)
1	30	Normal	yes (FR1)	yes (FR1)
2	60	Normal, extended	yes (FR1, FR2)	no
3	120	Normal	yes (FR2)	yes (FR2)
4	240	Normal	no	yes (FR2)

Table 12.1. *Spacing between sub-carriers*

The physical resource block (PRB) is made up of 12 consecutive sub-carriers. The minimum and maximum number of blocks in a radio channel depends on the spacing between the sub-carriers (Table 12.2), which determines the minimum and maximum bandwidth of the radio channel (Table 12.3).

Spacing between sub-carriers	PRB minimum number	PRB maximum number
15/30/60/120 kHz	24	275
240 kHz	24	138

Table 12.2. *PRB number*

Random access preamble sequences of two different lengths are supported by the physical random access channel (PRACH).

The long sequence length is applied with sub-carrier spacing of 1.25 kHz and 5 kHz. The short sequence length is applied with sub-carrier spacing of 15, 30, 60 and 120 kHz.

Spacing between sub-carriers	Minimum bandwidth (MHz)	Maximum bandwidth (MHz)
15 kHz	4.32	49.5
30 kHz	8.64	99
60 kHz	17.28	198
120 kHz	34.56	396
240 kHz	69.12	397.44

Table 12.3. *Radio channel bandwidth*

12.5.3. *Time frame*

Downlink and uplink are organized in frames which duration is equal to 10 ms duration, each frame consisting of ten sub-frames of 1 msec. Each frame is divided into two half-frames of size equal to five sub-frames:

– half-frame 0 is composed of sub-frames 0 to 4;

– half-frame 1 is composed of sub-frames 5 to 9.

For the LTE interface, the sub-frame is composed of two time slots. For the NR interface, the number of time slots in the sub-frame depends on the spacing between the sub-carriers (Table 12.4).

For the LTE interface, the value of the transmission time interval (TTI) corresponds to the duration of the sub-frame and has a fixed value equal to 1 ms. For the NR interface, the value of the TTI corresponds to the duration of the time slot and has a value that depends on the spacing between the sub-carriers (Table 12.4).

Spacing between sub-carriers	Number of slots per sub-frame	Number of slots per frame	TTI
15 kHz	1	10	1 ms
30 kHz	2	20	0.5 ms
60 kHz	4	40	0.25 ms
120 kHz	8	80	0.125 ms
240 kHz	16	160	0.0625 ms

Table 12.4. *Time frame structure*

For the LTE interface, the time slot includes seven OFDM symbols for the normal cyclic prefix and six OFDM symbols for the extended cyclic prefix.

For the NR interface, the time slot comprises 14 OFDM symbols for the normal cyclic prefix and 12 OFDM symbols for the extended cyclic prefix.

For the TDD mode, the elementary resource assigned to the downlink or uplink is different for the LTE and NR interfaces:

– for the LTE interface, the elementary resource corresponds to a sub-frame and seven configurations are defined;

– for the NR interface, the elementary resource corresponds to an OFDM symbol and 62 configurations are defined.

12.5.4. *Error correction codes*

The PDSCH and PUSCH use turbo code for the LTE interface and low-density parity check (LDPC) for the NR interface.

The PDCCH and PUCCH use tail-biting convolutional coding (TBCC) for the LTE interface and polar code for the NR interface.

12.5.5. *Reference signals*

For the LTE interface, the cell-specific reference signal (CRS) is used to demodulate the PBCH, PDSCH and PDCCH.

For the NR interface, the CRS is suppressed and the demodulation uses the demodulation reference signal (DMRS) dedicated to the physical channel. The number of DMRS symbols and the mapping to the resource elements are configured by the en-gNB entity.

The phase tracking reference signal (PTRS) may be transmitted over additional symbols to reduce the phase noise of the receiver oscillator when the frequency range FR2 is used.

12.5.6. *PSS, SSS and PBCH*

For the LTE interface and FDD mode, the PSS occupies the last symbol of time slots 0 and 10 on the time domain, and 62 sub-carriers on the frequency domain. The PSS is transmitted with a periodicity of 5 ms (Figure 12.11).

The SSS occupies the penultimate symbol of time slots 0 and 10 on the time domain, and 62 sub-carriers on the frequency domain. The PSS is transmitted with a periodicity of 5 ms (Figure 12.11).

The PBCH occupies the first four symbols of time slot 1 on the time domain, and 72 sub-carriers on the frequency domain. The PBCH is transmitted with a periodicity of 10 ms (Figure 12.11).

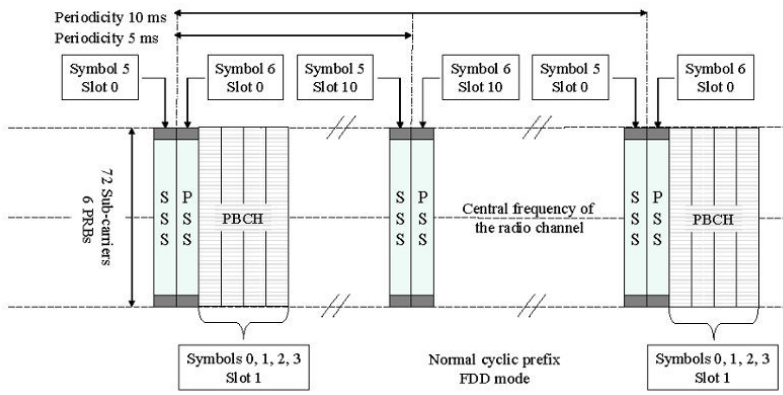

Figure 12.11. *PSS, SSS and PBCH location: LTE interface and TDD mode*

For the TDD mode, the PSS occupies the third symbol of time slots 2 and 12 on the time domain, and 62 sub-carriers on the frequency domain. The SSS occupies the last symbol of time slots 1 and 11 on the time domain, and 62 sub-carriers on the frequency domain.

For the NR interface, the PSS, SSS and PBCH form a block of four symbols. The PSS and SSS respectively occupy the first and third symbols of the block on the time domain and 127 sub-carriers on the frequency domain (Figure 12.12).

The PBCH occupies the last three symbols of the block on the time domain and, on the frequency domain, 240 sub-carriers for the second and the fourth symbol and 96 sub-carriers for the third symbol (Figure 12.12).

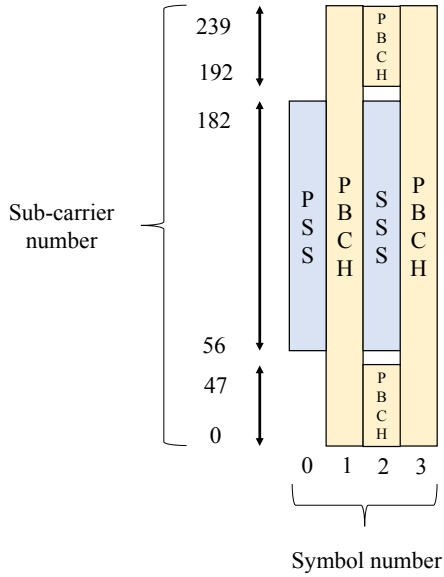

Figure 12.12. *Block of PSS, SSS and PBCH*

The blocks are transmitted in the first half-frame with a period of 20 ms. The maximum number of blocks in a half-frame is determined from the radio channel frequency:

– four blocks for frequencies less than or equal to 3GHz;

– eight blocks for frequencies between 3GHz and 6 GHz;

– 64 blocks for frequencies in FR2.

Each block is transmitted by a specific beam, radiated in a certain direction.

By way of example, Figure 12.13 describes the position of the four blocks for a spacing of 15 kHz and a frequency of less than or equal to 3GHz, the symbols being numbered from 0 to 69 for the first half-frame.

Table 12.5 shows the number of the first symbol of the block for the different values relating to the spacing between the sub-carriers and the radio channel frequency.

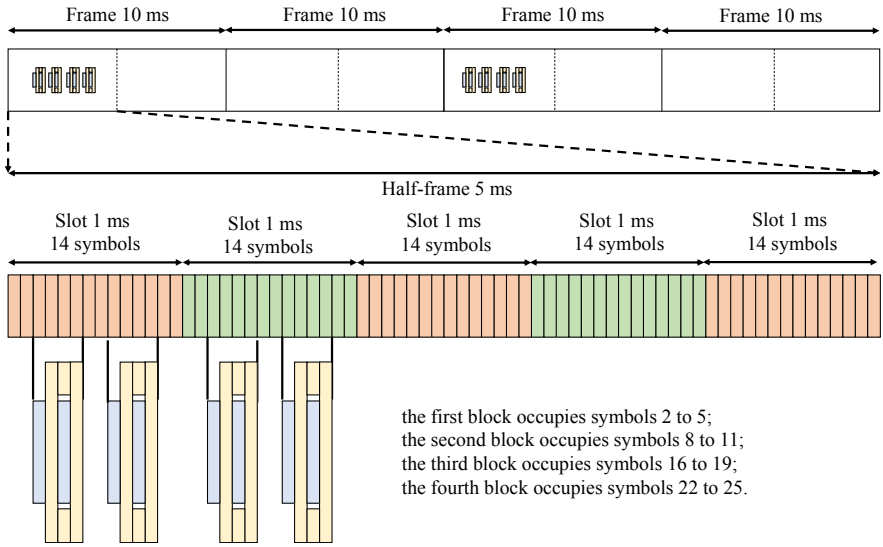

Figure 12.13. *PSS, SSS and PBCH location: NR interface*

Spacing between sub-carriers	f ≤ 3 GHz	3 GHz < f ≤ 6GHz	6 GHz < f
Case A 15 kHz	2, 8, 16, 22	2, 8, 16, 22, 30, 36, 44, 50	Not available
Case B 30 kHz	4, 8, 16, 20	4, 8, 16, 20 32, 36, 44, 48	Not available
Case C 30 kHz	2, 8, 16, 22	2, 8, 16, 22, 30, 36, 44, 50	Not available
Case D 120 kHz	Not available	Not available	{4, 8, 16, 20} + 28×n n = 0 to 15
Case E 240 kHz	Not available	Not available	{4, 8, 16, 20} + 28×n n = 0 to 15

Table 12.5. *PSS, SSS and PBCH location: NR interface*

References

General documentation

4G LTE Advanced Pro and The Road to 5G – Erik Dahlman, Stefan Parkvall, Johan Sköld – Elsevier – 2016.

From LTE to LTE-Advanced Pro and 5G – Moe Rahnema, Marcin Dryjanski – Artech House – 2017.

Inside 3GPP Release 13 – 4G Americas – 2016.

LTE-Advanced Pro Introduction – Rohde & Schwarz – 2017.

Mobile Broadband Evolution Toward 5G – 4G Americas – 2015.

Readers may find more detailed information about LTE and LTE Advanced technologies in the following books:

4G LTE / LTE-Advanced for Mobile Broadband – Erik Dahlman, Stefan Parkvall, Johan Sköld – Elsevier – 2011.

4G Mobile Broadband Evolution: 3GPP Release 10 and Beyond – HSPA1, SAE/LTE and LTE-Advanced – 4G Americas – 2011.

Introducing LTE-Advanced – Agilent Technologies – 2010.

Long Term Evolution IN BULLETS – Chris Johnson – 2012.

LTE-Advanced: Technology and Test Challenges – 3GPP Releases 10, 11, 12 and Beyond – Keysight Technologies – 2017.

LTE-Advanced Technology Introduction – Meik Kottkamp – Rohde & Schwarz – 2010.

LTE and LTE Advanced: 4G Network Radio Interface – André Perez – ISTE Ltd/ Wiley – 2016.

LTE et les réseaux 4G – Yannick Bouguen, Eric Hardouin, François-Xavier Wolff – Eyrolles – 2012.

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

MIMO and Smart Antennas for Mobile Broadband Networks – 4G Americas – 2013.

Wi-Fi Integration to the 4G Mobile Network – André Perez – ISTE Ltd/ Wiley – 2018.

Radio interface specifications for LTE, LTE Advanced and LTE Advanced Pro

[3GPP TS 36.211] Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation.

[3GPP TS 36.212] Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding.

[3GPP TS 36.213] Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures.

[3GPP TS 36.300] Terrestrial Radio Access Network (E-UTRAN); Overall description.

[3GPP TS 36.321] Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification.

[3GPP TS 36.322] Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification.

[3GPP TS 36.323] Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification.

[3GPP TS 36.331] Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC).

Chapter 1: MBB Service – Network Architecture
Chapter 2: MBB Service – Spatial Multiplexing
Chapter 3: MBB Service – Carrier Aggregation

[3GPP TR 36.897] Elevation Beamforming/Full-Dimension (FD) MIMO for LTE.

[3GPP TS 23.214] Architecture enhancements for control and user plane separation of EPC nodes.

[3GPP TS 23.401] General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.

[3GPP TS 23.830] Architecture aspects of Home NodeB and Home eNodeB.

[3GPP TS 36.401] Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Architecture description.

Long Term Evolution (LTE) and LTE-Advanced Activities in Small Cell Networks – Qi Jiang, Jinsong Wu, Lu Zhang, Shengjie Zhao – *Design and Deployment of Small Cell Networks* – Alagan Anpalagan, Mehdi Bennis, Rath Vannithamby (eds) – 2016.

LTE Advanced Release 13 Multiple Antenna Technologies and Improved Reception Technologies – Yosuke Sano, Atsushi Fukuda, Sukuru Okuyama, Yuichi Kakishima, Chongning Na – *NTT DOCOMO Technical Reports Journal*, vol. 18, no. 2 – 2016.

LTE Aggregation & Unlicensed Spectrum – 5G Americas – 2015.

LTE Carrier Aggregation – 4G Americas – 2014.

LTE Small Cell Enhancement by Dual Connectivity – Jian Zhang, Qinghai Zeng, Mahmoodi Toktam, Andreas Georgakopoulos, Panagiotis Demestichas – Wireless Word Research Forum – 2014.

LTE Transmission Modes and Beamforming – Bernhard Schulz – Rohde & Schwarz – 2015.

MIMO and Smart Antennas for Mobile Systems – 4G Americas – 2012.

Chapter 4: Wi-Fi Integration – Network Architecture
Chapter 5: Wi-Fi Integration – Procedures
Chapter 6: Wi-Fi Integration – Network Discovery and Selection

[3GPP TS 23.402] Architecture enhancements for non-3GPP accesses.

[3GPP TS 24.302] Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks.

[3GPP TS 24.312] Access Network Discovery and Selection Function (ANDSF); Management Object (MO).

[3GPP TS 29.273] Evolved Packet System (EPS); 3GPP EPS AAA interfaces.

Analysis of LTE / Wi-Fi Aggregation Solutions – Netmanias – 2016.

Hotspot 2.0 (Release 2) Technical Specification – Wi-Fi Alliance – 2016.

Integration of Cellular and Wi-Fi Networks – 4G Americas – 2013.

Network Architecture for LTE and Wi-Fi Interworking – Chris Yoo – Netmanias – 2012.

Wi-Fi Roaming Guidelines – GSMA – IR.61 – 2015.

WLAN Traffic Offload in LTE – A. Schumacher, J. Schlienz – Rohde & Schwarz – 2012.

Chapter 7: LLC Service – Proximity Communications
Chapter 8: LLC Service – Group Communications
Chapter 9: LLC Service – GCSE and MCPTT Functions

[3GPP TS 23.179] Functional architecture and information flows to support mission critical communication services; Stage 2.

[3GPP TS 23.246] Multimedia Broadcast/Multicast Service (MBMS): Architecture and functional description.

[3GPP TS 23.285] Architecture enhancements for V2X Services.

[3GPP TS 23.303] Proximity-based services (ProSe); Stage 2.

[3GPP TS 23.468] Group Communication System Enablers for LTE (GCSE_LTE); Stage 2.

[3GPP TS 33.179] Security of Mission Critical Push To Talk (MCPTT) over LTE.

A New 5G Technology for Short-Range Vehicle-to-Everything Communications – Rafael Molina-Masegosa, Javier Gonzalvez – *IEEE Vehicular Technology Magazine* – 2017.

Device to Device Communication in LTE – J. Schlienz, A. Roessler – Rohde & Schwarz – 2015.

Introduction to the vehicle-to-everything communications service V2X – Rohde & Schwarz.

LTE for Public Safety – Rainer Liebhart, Devaki Chandramouli, CurtWong, Jürgen Merkel – Wiley – 2015.

Mobile Broadband Communications for Public Safety – Ramon Ferrús, Oriol Sallent – Wiley – 2015.

Network 2020: 4G The Broadcasting Opportunity – GSMA.

Network 2020: Mission Critical Communications – GSMA.

Chapter 10: MTC Service – Network Architecture
Chapter 11: MTC Service – Radio Interfaces

[3GPP TS 22.368] Service requirements for Machine Type Communications (MTC).

[3GPP TS 23.682] Architecture enhancements to facilitate communications with packet data networks and applications.

3GPP Low Power Wide Area Technologies – GSMA.

Core Network Infrastructure and Congestion Control Technology for M2M Communications – Kaisuke Sasada, Itsuma Tanaka, Takashi Koshimizu – *NTT DOCOMO Technical Reports Journal*, vol. 15, no. 2 – 2013.

LTE Progress Leading to the 5G Massive Internet of Things – 5G Americas – 2017.

LTE-M Deployment Guide to Basic Feature Set Requirements – GSMA – 2018.

Narrowband Internet of Things – J. Schlienz, D. Raddino – Rohde & Schwarz – 2016.

NarrowBand IoT Data Transmission Procedures for Massive Machine Type Communications – Pilar Andres-Maldonado, Pablo Ameigeiras, Jonathan Prados-Garzon, Jorge Navarro-Ortiz, Juan M. Lopez-Soler – *IEEE Network Magazine* – 2017.

NarrowBand-IoT: A Survey on Downlink and Uplink Perspectives – Luca Feltrin, Galini Tsoukaneri, Massimo Condoluci, Chiara Buratti, Toktam Mahmoodi, Mischa Dohler, Roberto Verdone – *IEEE Wireless Communications Magazine* – 2018.

NB-IoT Deployment Guide to Basic Feature set Requirements – GSMA – 2018.

New technologies for achieving IoT in LTE Release 13 – Kasuaki Takeda, Wuri A. Hapsari, Hideaki Takahashi, Daisuke Fujishima, Zhen Miao – *NTT DOCOMO Technical Reports Journal*, vol. 18, no. 2 – 2016.

Chapter 12: MBB Service – 5G Integration

[3GPP TR 38.802] Study on New Radio Access Technology Physical Layer Aspects.

[3GPP TS 37.340] NR; Multi-connectivity Overall Description Stage 2.

[3GPP TS 38.300] NR Overall Description.

[3GPP TS 38.912] Study on New Radio (NR) access technology.

5G Radio Access Network Standardization Trends – Anil Umesh, Wuri A. Hapsari, Toru Ushino, Teruaki Toeda, Hideaki Takahashi – *NTT DOCOMO Technical Reports Journal*, vol. 19, no. 3 – 2018.

Common Public Radio Interface: eCPRI Interface Specification – 2017.

Road to 5G: Introduction and Migration – GSMA.

Index

LTE Advanced Pro: Towards the 5G Mobile Network,
First Edition. Frédéric Launay and André Perez.

D, E, F

G, H, I

L, M, N

O, P, Q

R, S, T

U, V, W, X

Other titles from

in

Networks and Telecommunications

2018

ANDIA Gianfranco, DURO Yvan, TEDJINI Smail
Non-linearities in Passive RFID Systems: Third Harmonic Concept and Applications

BOUILLARD Anne, BOYER Marc, LE CORRONC Euriell
Deterministic Network Calculus: From Theory to Practical Implementation

PEREZ André
Wi-Fi Integration to the 4G Mobile Network

2017

BENSLAMA Malek, BENSLAMA Achour, ARIS Skander
Quantum Communications in New Telecommunications Systems

HILT Benoit, BERBINEAU Marion, VINEL Alexey, PIROVANO Alain
Networking Simulation for Intelligent Transportation Systems: High Mobile Wireless Nodes

LESAS Anne-Marie, MIRANDA Serge
The Art and Science of NFC Programming
(Intellectual Technologies Set – Volume 3)

2016

AL AGHA Khaldoun, PUJOLLE Guy, ALI-YAHIYA Tara
Mobile and Wireless Networks
(Advanced Network Set – Volume 2)

BATTU Daniel
Communication Networks Economy

BENSLAMA Malek, BATATIA Hadj, MESSAI Abderraouf
Transitions from Digital Communications to Quantum Communications: Concepts and Prospects

CHIASSERINI Carla Fabiana, GRIBAUDO Marco, MANINI Daniele
Analytical Modeling of Wireless Communication Systems
(Stochastic Models in Computer Science and Telecommunication Networks Set – Volume 1)

EL FALLAH SEGHROUCHNI Amal, ISHIKAWA Fuyuki, HÉRAULT Laurent, TOKUDA Hideyuki
Enablers for Smart Cities

PEREZ André
VoLTE and ViLTE

2015

BENSLAMA Malek, BATATIA Hadj, BOUCENNA Mohamed Lamine
Ad Hoc Networks Telecommunications and Game Theory

BENSLAMA Malek, KIAMOUCHE Wassila, BATATIA Hadj
Connections Management Strategies in Satellite Cellular Networks

BERTHOU Pascal, BAUDOIN Cédric, GAYRAUD Thierry, GINESTE Matthieu
Satellite and Terrestrial Hybrid Networks

CUADRA-SANCHEZ Antonio, ARACIL Javier
Traffic Anomaly Detection

LE RUYET Didier, PISCHELLA Mylène
Digital Communications 1: Source and Channel Coding

PEREZ André
LTE and LTE Advanced: 4G Network Radio Interface

PISCHELLA Mylène, LE RUYET Didier
Digital Communications 2: Digital Modulations

PUJOLLE Guy
Software Networks
(Advanced Network Set – Volume 1)

2014

ANJUM Bushra, PERROS Harry
Bandwidth Allocation for Video under Quality of Service Constraints

BATTU Daniel
New Telecom Networks: Enterprises and Security

BEN MAHMOUD Mohamed Slim, GUERBER Christophe, LARRIEU Nicolas, PIROVANO Alain, RADZIK José
Aeronautical Air−Ground Data Link Communications

BITAM Salim, MELLOUK Abdelhamid
Bio-inspired Routing Protocols for Vehicular Ad-Hoc Networks

CAMPISTA Miguel Elias Mitre, RUBINSTEIN Marcelo Gonçalves
Advanced Routing Protocols for Wireless Networks

CHETTO Maryline
Real-time Systems Scheduling 1: Fundamentals
Real-time Systems Scheduling 2: Focuses

EXPOSITO Ernesto, DIOP Codé
Smart SOA Platforms in Cloud Computing Architectures

MELLOUK Abdelhamid, CUADRA-SANCHEZ Antonio
Quality of Experience Engineering for Customer Added Value Services

OTEAFY Sharief M.A., HASSANEIN Hossam S.
Dynamic Wireless Sensor Networks

PEREZ André
Network Security

PERRET Etienne
Radio Frequency Identification and Sensors: From RFID to Chipless RFID

REMY Jean-Gabriel, LETAMENDIA Charlotte
LTE Standards
LTE Services

TANWIR Savera, PERROS Harry
VBR Video Traffic Models

VAN METER Rodney
Quantum Networking

XIONG Kaiqi
Resource Optimization and Security for Cloud Services

2013

ASSING Dominique, CALÉ Stéphane
Mobile Access Safety: Beyond BYOD

BEN MAHMOUD Mohamed Slim, LARRIEU Nicolas, PIROVANO Alain
Risk Propagation Assessment for Network Security: Application to Airport Communication Network Design

BERTIN Emmanuel, CRESPI Noël
Architecture and Governance for Communication Services

BEYLOT André-Luc, LABIOD Houda
Vehicular Networks: Models and Algorithms

BRITO Gabriel M., VELLOSO Pedro Braconnot, MORAES Igor M.
Information-Centric Networks: A New Paradigm for the Internet

DEUFF Dominique, COSQUER Mathilde
User-Centered Agile Method

DUARTE Otto Carlos, PUJOLLE Guy
Virtual Networks: Pluralistic Approach for the Next Generation of Internet

FOWLER Scott A., MELLOUK Abdelhamid, YAMADA Naomi
LTE-Advanced DRX Mechanism for Power Saving

JOBERT Sébastien *et al.*
Synchronous Ethernet and IEEE 1588 in Telecoms: Next Generation Synchronization Networks

MELLOUK Abdelhamid, HOCEINI Said, TRAN Hai Anh
Quality-of-Experience for Multimedia: Application to Content Delivery Network Architecture

NAIT-SIDI-MOH Ahmed, BAKHOUYA Mohamed, GABER Jaafar, WACK Maxime
Geopositioning and Mobility

PEREZ André
Voice over LTE: EPS and IMS Networks

2012

AL AGHA Khaldoun
Network Coding

BOUCHET Olivier
Wireless Optical Communications

DECREUSEFOND Laurent, MOYAL Pascal
Stochastic Modeling and Analysis of Telecoms Networks

DUFOUR Jean-Yves
Intelligent Video Surveillance Systems

EXPOSITO Ernesto
Advanced Transport Protocols: Designing the Next Generation

JUMIRA Oswald, ZEADALLY Sherali
Energy Efficiency in Wireless Networks

KRIEF Francine
Green Networking

PEREZ André
Mobile Networks Architecture

2011

BONALD Thomas, FEUILLET Mathieu
Network Performance Analysis

CARBOU Romain, DIAZ Michel, EXPOSITO Ernesto, ROMAN Rodrigo
Digital Home Networking

CHABANNE Hervé, URIEN Pascal, SUSINI Jean-Ferdinand
RFID and the Internet of Things

GARDUNO David, DIAZ Michel
Communicating Systems with UML 2: Modeling and Analysis of Network Protocols

LAHEURTE Jean-Marc
Compact Antennas for Wireless Communications and Terminals: Theory and Design

PALICOT Jacques
Radio Engineering: From Software Radio to Cognitive Radio

PEREZ André
IP, Ethernet and MPLS Networks: Resource and Fault Management

RÉMY Jean-Gabriel, LETAMENDIA Charlotte
Home Area Networks and IPTV

TOUTAIN Laurent, MINABURO Ana
Local Networks and the Internet: From Protocols to Interconnection

2010

CHAOUCHI Hakima
The Internet of Things

FRIKHA Mounir
Ad Hoc Networks: Routing, QoS and Optimization

KRIEF Francine
Communicating Embedded Systems / Network Applications

2009

CHAOUCHI Hakima, MAKNAVICIUS Maryline
Wireless and Mobile Network Security

VIVIER Emmanuelle
Radio Resources Management in WiMAX

2008

CHADUC Jean-Marc, POGOREL Gérard
The Radio Spectrum

GAÏTI Dominique
Autonomic Networks

LABIOD Houda
Wireless Ad Hoc and Sensor Networks

LECOY Pierre
Fiber-optic Communications

MELLOUK Abdelhamid
End-to-End Quality of Service Engineering in Next Generation Heterogeneous Networks

PAGANI Pascal *et al.*
Ultra-wideband Radio Propagation Channel

2007

BENSLIMANE Abderrahim
Multimedia Multicast on the Internet

PUJOLLE Guy
Management, Control and Evolution of IP Networks

SANCHEZ Javier, THIOUNE Mamadou
UMTS

VIVIER Guillaume
Reconfigurable Mobile Radio Systems