LTE

3GPP Standard Perspective
Chapter 1 - Introduction

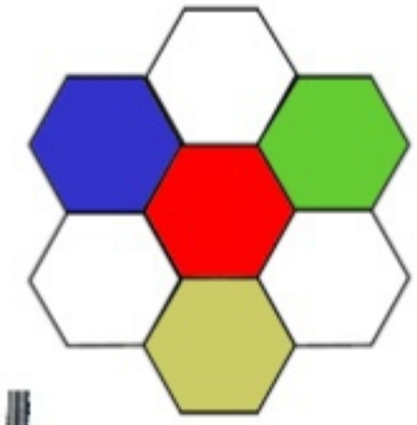
Muhannad Aulama

Contents of Chapter 1

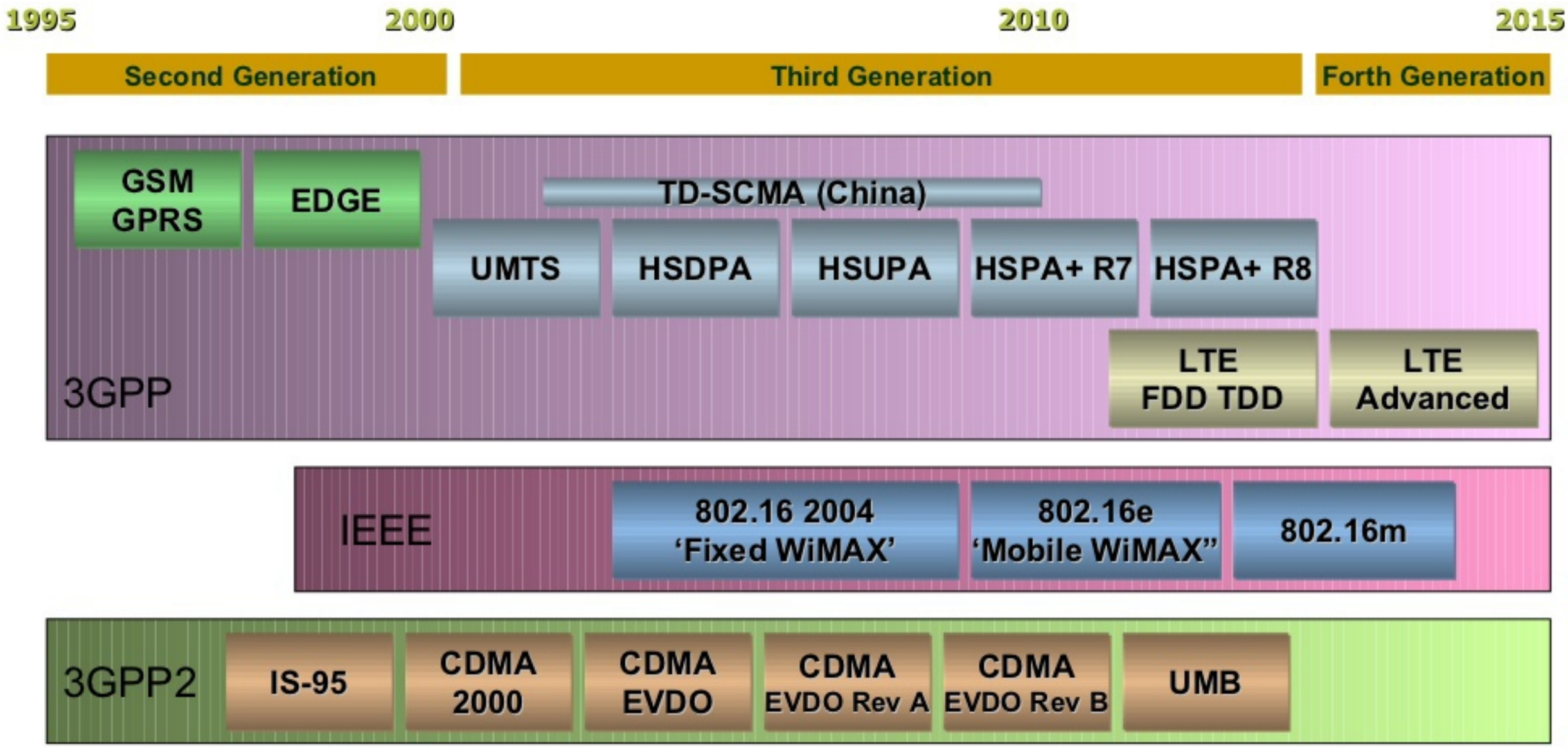
- History.
- Mobile Communications Standard Timeline.
- Regulators vs Technology.
- 3GPP Evolution.
- 3GPP Standardization Process.
- Requirements and Targets for LTE.
- LTE Frequency Bands and Channel Bandwidth.
- Technologies for LTE:
  - Multi-carrier Technology.
  - Multiple Antenna Technology.
  - Evolved Packet System.
  - Evolved Packet Core.
  - User Equipment Capability.

History

- The Long Term Evolution (LTE) is just one of the latest steps in an advancing series of mobile telecommunication systems:
  - **Cells**: The series began in 1947 with the development of the concept *cells* by the famous Bell Labs.
  - **First Generation**: The first mobile communication systems to see large-scale commercial growth arrived in the 1980s and became known as the "First Generation. It comprised of a number of independently-developed systems worldwide: AMPS in America, TACS in Europe, J-TACS in Japan.
  - **GSM**: Global roaming first became a possibility with the development of the digital "Second Generation" system known as GSM. GSM is a robust, interoperable, and widely accepted standard thanks to the collaboration of a number of companies working together under the European Telecommunications Standard Institute (ETSI).



Mobile Communications Standard Timeline



Regulators vs Technology

Aggregated Data Rate = Bandwidth x Spectral Efficiency

Regulation & Licenses
(ITU-R, regional regulators)

Technology & Standards
(UMTS, HSPA+, LTE)

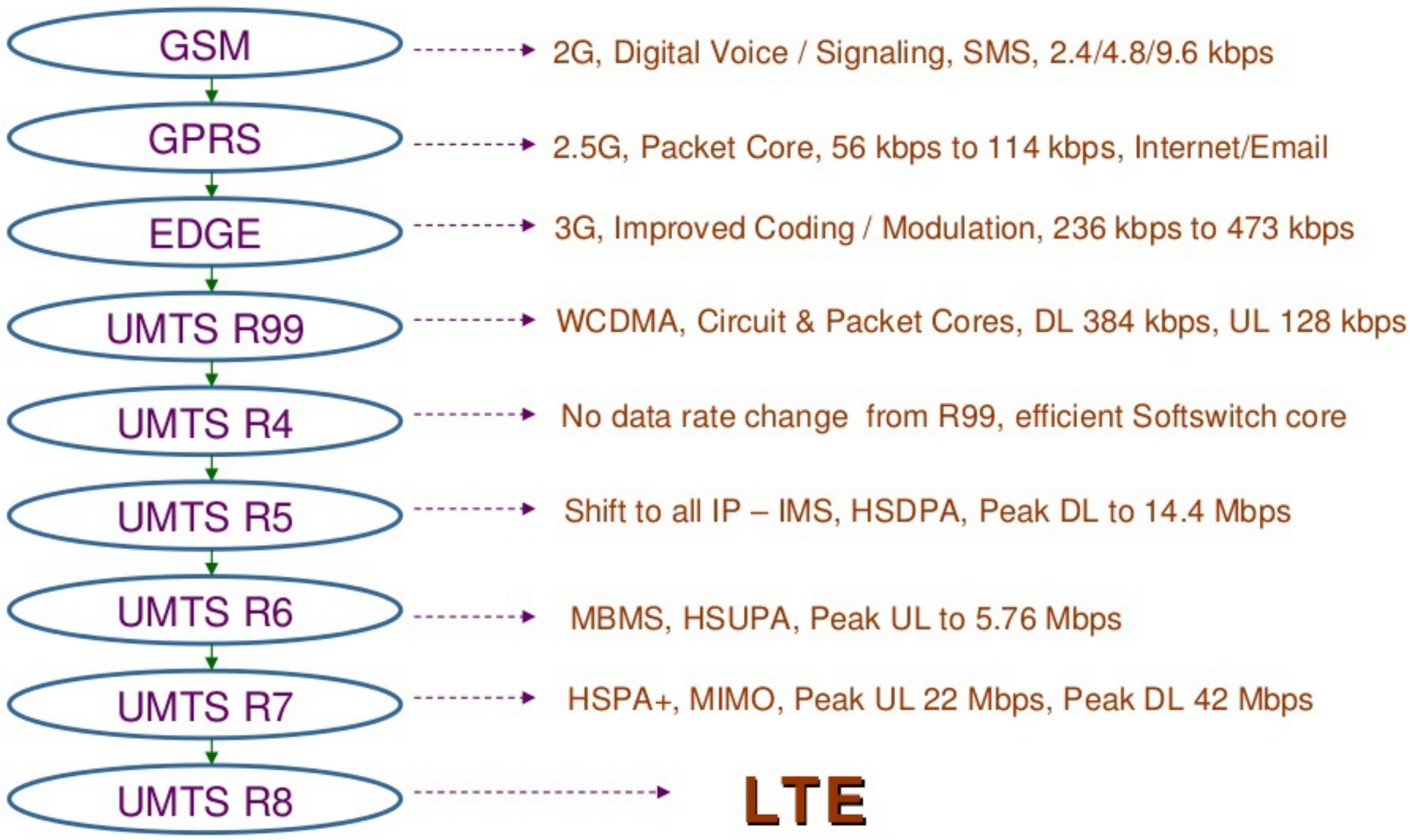
International Telecommunication Union – Radio (ITU-R)

3GPP
UMTS
HSDPA
HSPA+
LTE

IEEE
Fixed & Mobile WiMAX

3GPP2
CDMA 2000
CDMA EDVO

3GPP Evolution



3GPP Standardization Process

- The collaboration for both GSM and UMTS was expanded beyond ETSI to encompass regional organizations from Japan (ARIB & TCC), Korea (TTA), North America (ATIS) and China (CCSA).
- All Documents submitted to 3GPP are publicly available on 3GPP website: http://www.3gpp.org
- In reaching consensus around a technology, 3GPP working groups (WGs) take into account performance, implementation cost, complexity and compatibility. Therefore, formal voting is rare in 3GPP to avoid polarization of companies.

- The LTE standardization process was inaugurated at a workshop in Toronto in November 2004, when a broad range of companies involved in the mobile communications presented their visions for the future evolution of 3GPP.

Requirements and Targets for LTE

Requirement	Current Release (Rel-6)	LTE
Peak Data Rate	14Mbps DL / 5.76Mbps UL	100Mbps DL/ 50 Mbps UL
Spectral Efficiency	0.6 - 0.8 DL / 0.35 UL (bps/Hz/sector)	3 - 4x DL / 2 - 3x UL Improvement
5% Packet Call Throughput	64Kbps DL / 5 Kbps UL	3 - 4x DL / 2 - 3x UL Improvement
Average User Throughput	900Kbps DL / 150 Kbps UL	3 - 4x DL / 2 - 3x UL Improvement
User Plane Latency	50 msec	5 msec
Call Setup Time	2 sec	50 msec
Broadcast Data Rate	384 Kbps	6 - 8x Improvement
Mobility	Up to 250 Km/h	Up to 350 Km/h
Multi-antenna support	No	Yes
Bandwidth	5MHz	Up to 20MHz

Requirements and Targets for LTE

- Peak Data Rate: Assuming 20MHz bandwidth with spectral efficiency of 5 DL and 2.5 UL bps/Hz, UE has two receive antennas and one transmit antenna.
- Mobility and Cell Range: LTE is required to support terminals moving at 350 km/h. LTE cells have radius up to 5 km, while for wide-area deployments cell range can go up to 100 km.
- Broadcast Mode Performance: LTE is required to integrate an efficient broadcast mode for high rate Multimedia Broadcast/Multicast Services (MBMS) such as Mobile TV based on a Single Frequency Network mode of operation.
- User Plane Latency: The average time between the first transmission of a data packet and the reception of a physical later ACK including HARQ retransmission rates.
- Control Plane Latency: The time required for performing the transition between RRC_IDLE to RRC_Connected.
- Spectrum Allocation and Duplex Modes: Spectrum Bandwidth from 1.4 MHz to 20 MHz, both FDD and TDD with wide range of frequency bands.
- Inter-working with other Radio Access Technologies: LTE allows interoperation with 3GPP technologies (GSM/EDGE, UTRAN) as well as non-3GPP technologies (WiFi, CDMA2000, WiMAX).

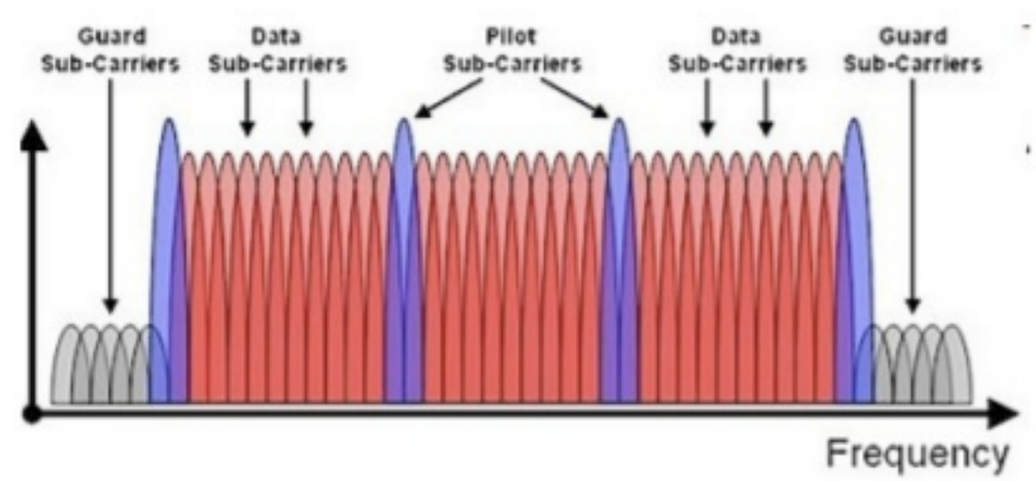
LTE Frequency Bands and Channel Bandwidth

- LTE operating bands include new spectrum, as well as the opportunity to re-farm existing legacy spectrum.
- It supports both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) air interface schemes. FDD requires paired frequencies, one for downlink and one for uplink, while TDD shares the same frequency for downlink and uplink.
- Various channel bandwidths are available in LTE technology allowing for spectrum flexibility. 1.4, 3, 5, 10, 15, and 20 MHz channel BW are available.

LTE Frequency Bands and Channel Bandwidth

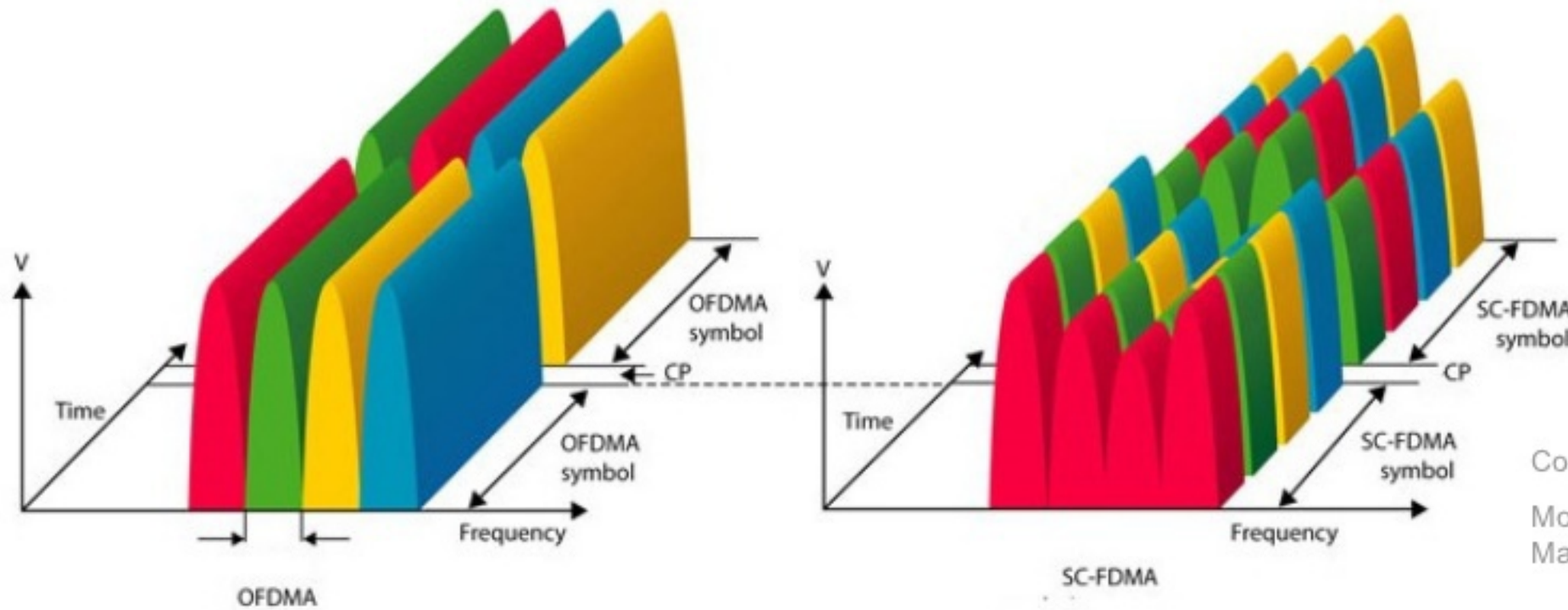
LTE Band	UL Freq Band (MHz)	DL Freq Band (MHz)	Duplex Mode
1	1920-1980	2110-2170	FDD
2	1850-1910	1930-1990	FDD
3	1710-1785	1805-1880	FDD
4	1710-1755	2110-2155	FDD
5	824-849	869-894	FDD
6	830-840	875-885	FDD
7	2500-2570	2620-2690	FDD
8	880-915	925-960	FDD
9	1749.9-1784.9	1844.9-1879.9	FDD
⋮	⋮		⋮
38	2570-2620		TDD
39	1880-1920		TDD
40	2300-2400		TDD

	Channel Bandwidth					
	1.4 MHz	3 MHz	5 MHz	10 MHz	15 MHz	20 MHz
Sampling Frequency (MHz)	1.92	3.84	7.68	15.36	23.04	30.72
Number of Subcarriers (FFT size)	128	256	512	1024	1536	2048
Subcarrier Spacing (kHz)	15 (7.5 used in MBMS-dedicated cell)					
Number of Occupied Subcarriers (data and reference, not DC or guard)	72	180	300	600	900	1200
Subframe Duration (ms)	1					
Number of Resource Blocks (per slot)	6	15	25	50	75	100
Number of OFDM symbols per subframe (Short/Long CP)	14/12					



Technologies for LTE: Multi-carrier Technology

- The first major design choice for LTE is the Multi-carrier OFDMA radio interface for DL, and SC-FDMA for UL.



Courtesy of:

MobileDevDesign Magazine

- OFDM subdivides the bandwidth available for signal transmission into a multitude of narrow band subcarriers, arranged to be mutually orthogonal. In OFDMA, this subdivision of the available bandwidth is exploited in sharing the subscribers among multiple users.

Technologies for LTE: Multi-carrier Technology

- Advantages of OFDMA:
  - Bandwidth Flexibility: Different spectrum bandwidths can be utilized without changing the fundamental system parameters or equipment design.
  - Multi-user Efficiency: Transmission resources of variable bandwidth can be allocated to different users and scheduled freely in the frequency domain.
  - Ease of Frequency Reuse: Fractional frequency reuse and interference coordination between cells are facilitated.
  - Robustness in Multi-path Environment: Thanks to the subdivision of the wide-band signal into multiple narrowband subcarriers, enabling inter-symbol interference to be largely constrained within a guard interval at the beginning of each symbol.
  - Low Complexity Receivers: By exploiting frequency domain equalization.
- Disadvantages of OFDAMA:
  - High PAPR: The transmitter design for OFDM is more costly, as the Peak-to-Average Power Ratio (PAPR) of an OFDM is relatively high, resulting in a need for a highly-linear RF power amplifier. This is not an issue for base stations, but is a serious problem for mobile terminal. Therefore, SC-FDMA is used in the uplink because it has lower PAPR.

Technologies for LTE: Multiple Antenna Technology

- The Use of multiple antenna technology allows the exploitation of spatial-domain as another new dimension:

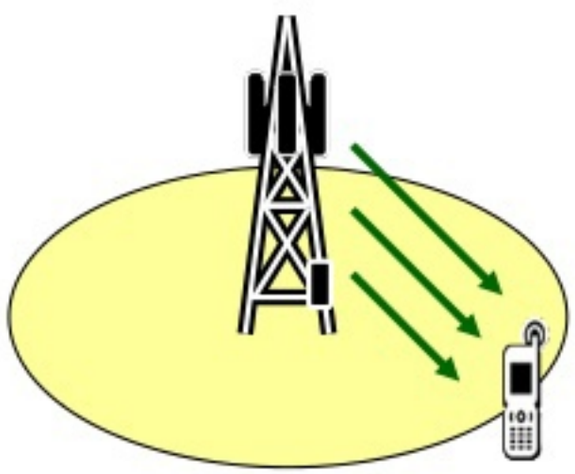
Air Interface Dimensions = Time + Frequency + Space

- Multiple Antennas can be used in a variety of ways, mainly based on three fundamental principles:
  - Diversity Gain: Use of the space-diversity provided by the multiple antennas to improve the robustness of the transmission against multipath fading.
  - Array gain: Concentration of energy in one or more given directions via precoding or beamforming. This also allows multiple users located in different directions to be served simultaneously (so called Multi-user MIMO).
  - Spatial Multiplexing Gain: Transmission of multiple signal streams to a single user on multiple spatial layers created by combinations of the available antennas.

Technologies for LTE: Multiple Antenna Technology

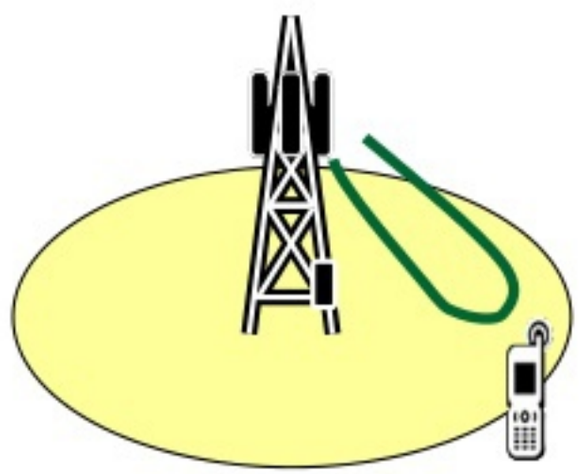
Diversity Gain

Same bit pattern transmitted over antennas



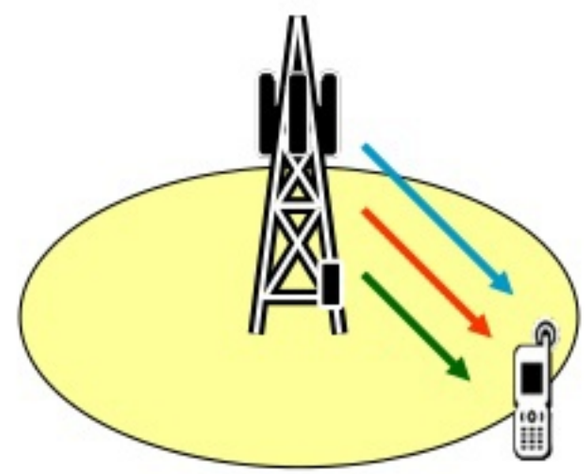
Array Gain

High energy received at mobile station

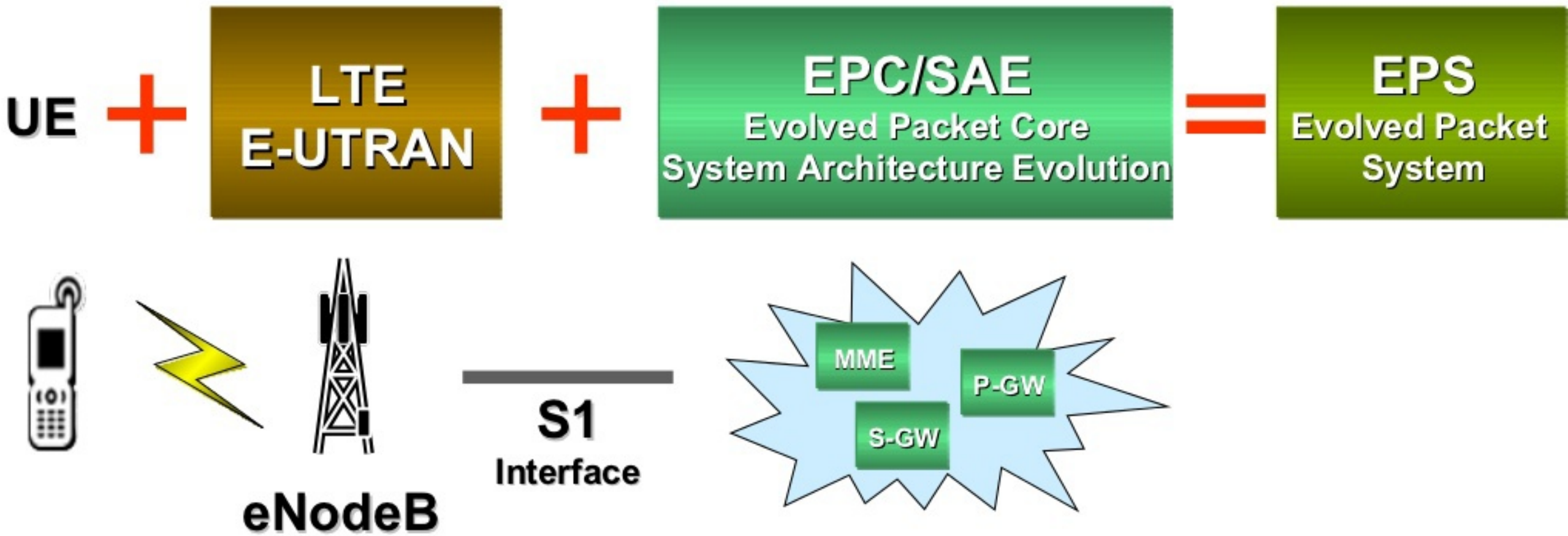


Spatial Multiplexing Gain

Different bit patterns transmitted over antennas

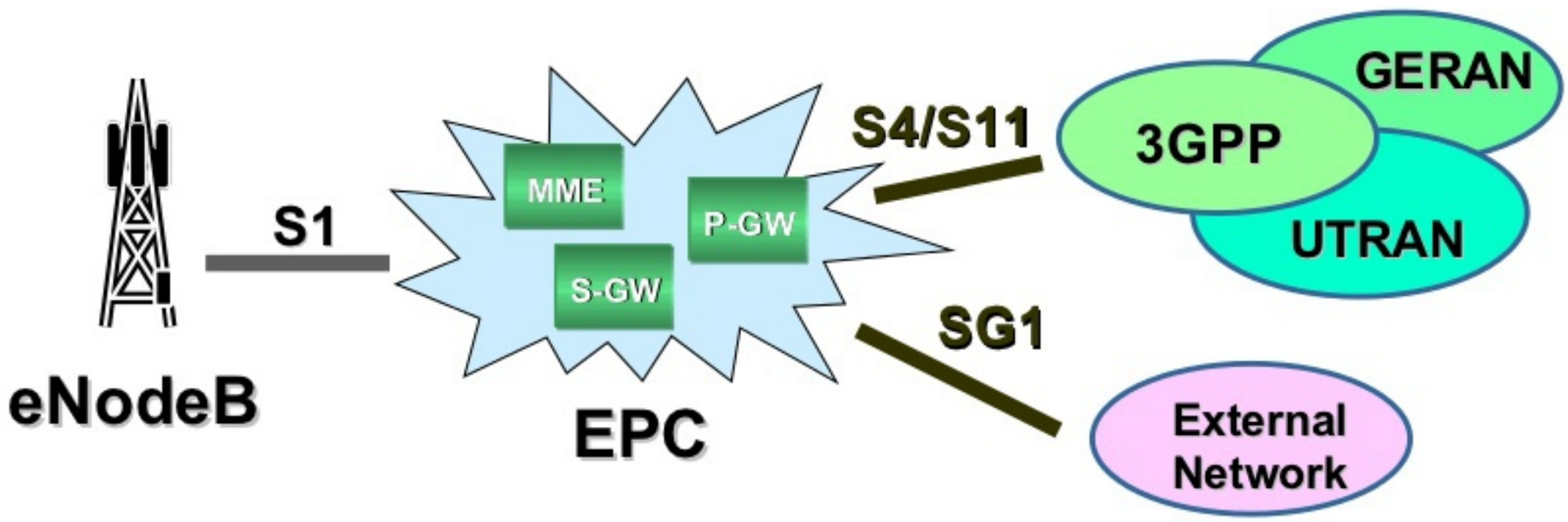


Technologies for LTE: Evolved Packet System



Technologies for LTE: Evolved Packet Core

- All IP flat network architecture: Optimal for LTE as a completely packet-oriented multi-service system.
- E-UTRAN is one single element: the eNodeB.
- Open and standardized interfaces.
- Interoperable with previous 3GPP technologies (GSM, UMTS) and non-3GPP technologies (WiFi, WiMAX).



Technologies for LTE: User Equipment Capability

- The LTE system has been designed to support a compact set of five categories of UE, ranging from relatively low-cost terminals with similar capabilities of UMTS HSPA, up to very high-capability terminals which exploit LTE to the max.

	UE Category				
	1	**2**	**3**	**4**	**5**
Maximum DL data rate (Mbps)	10	50	100	150	300
Maximum UL data rate (Mbps)	5	25	50	50	75
Number of receive antennas required	2	2	2	2	4
Number of downlink MIMO stream supported	1	2	2	2	4
Support for 64QAM modulation in DL	Yes	Yes	Yes	Yes	Yes
Support for 64QAM modulation in UL	No	No	No	No	Yes
Relative memory requirement (relative to cat 1)	1	4.9	4.9	7.3	14.6

Further Reading

- 3GPP Technical Report 25.814, “Physical Layer Aspects for Evolved UTRA (Release 7)”, www.3gpp.org.
- 3GPP Technical Report 25.913, “Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN) (Release 7)”, www.3gpp.org.

LTE

3GPP Standard Perspective
Chapter 2 – Network Architecture

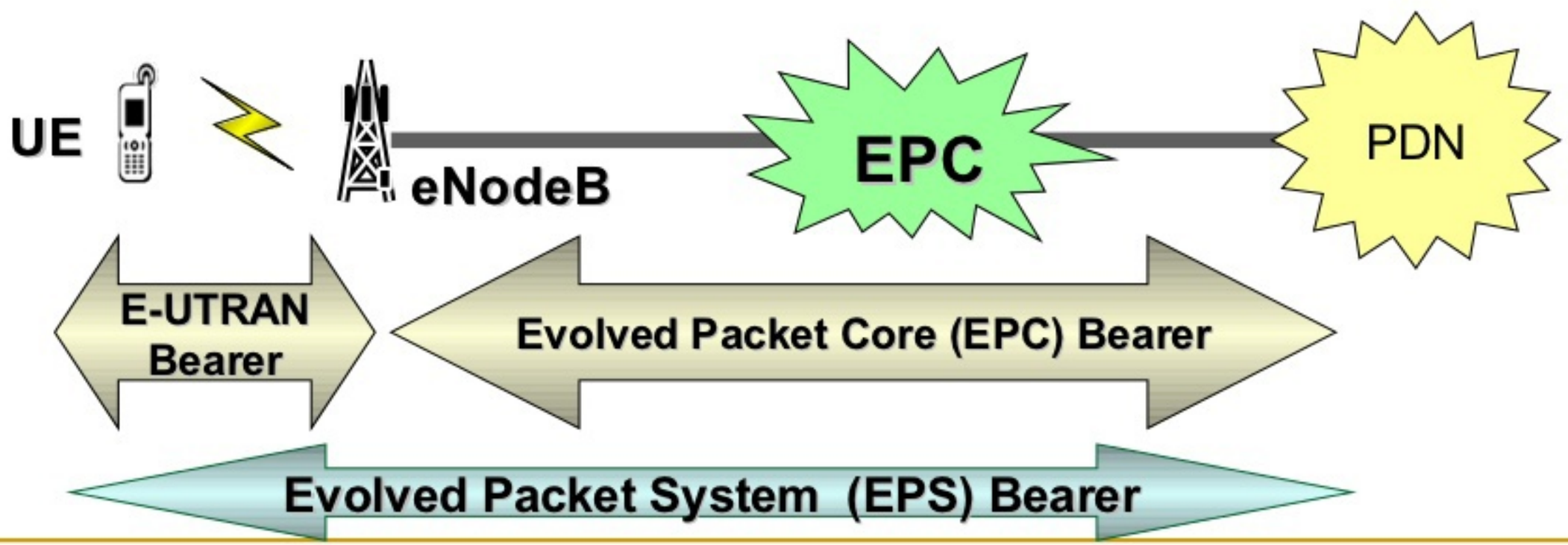
Muhannad Aulama

Contents of Chapter 2

- Introduction.
- LTE Architecture Overview
- E-UTRAN vs EPC .
- The Core Network.
- Non Access Startum (NAS) Procedures.
- The Access Network
- Roaming Architecture.
- Inter-Working with other Networks.
- Protocol Architecture: User Plane.
- Protocol Architecture: Control Plane.
- Quality of Service.
- Standardized QCI.
- EPS bearer mapping.
- Default Bearer Establishment.
- Bearer Establishment Procedure.
- The S1 Interface: Control Plane.
- The S1 Interface: User Plane.
- S1 Interface Procedures.
- S1 Topology
- S1-based Handover.
- X2 Interface
- X2 Interface Procedures
- Seamless vs Lossless Handover
- X2-based Handover Procedure

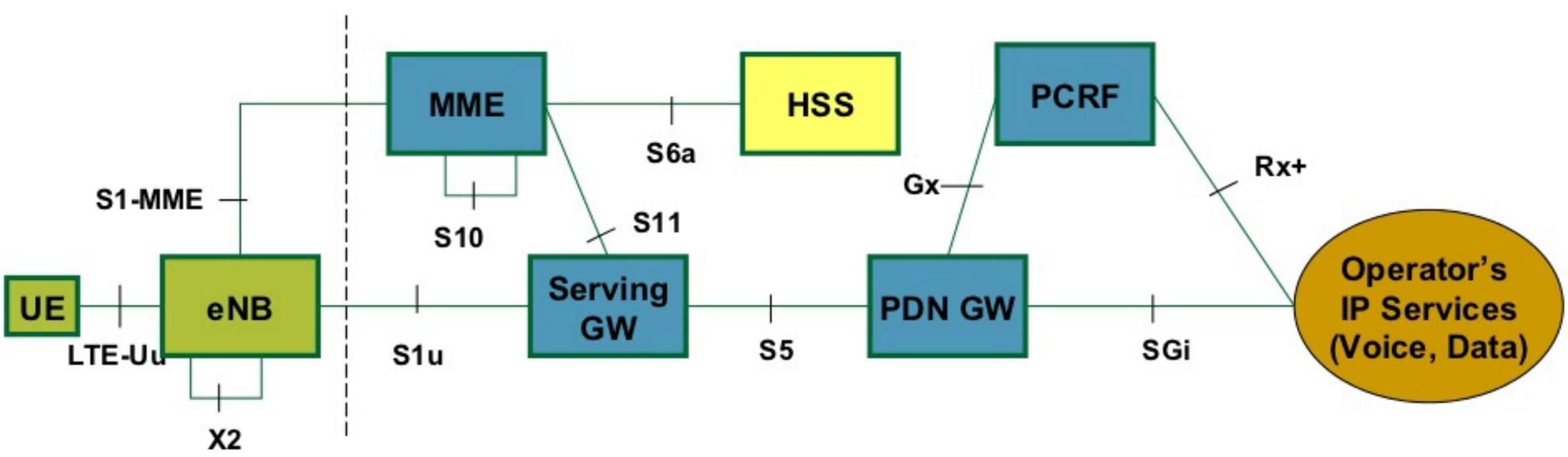
Introduction

- LTE has been designed to support only packet-switched services, in contrast to the circuit-switched model of previous cellular systems.
- LTE provides the user with IP connectivity to a PDN for accessing the internet, as well as for running services such as Voice over IP (VoIP).
- Evolved Packet System (EPS) uses the concept of EPS bearers to route IP traffic from gateway in the PDN to the UE. A bearer is an IP packet flow with a defined Quality of Service (QoS) between the gateway and the UE.

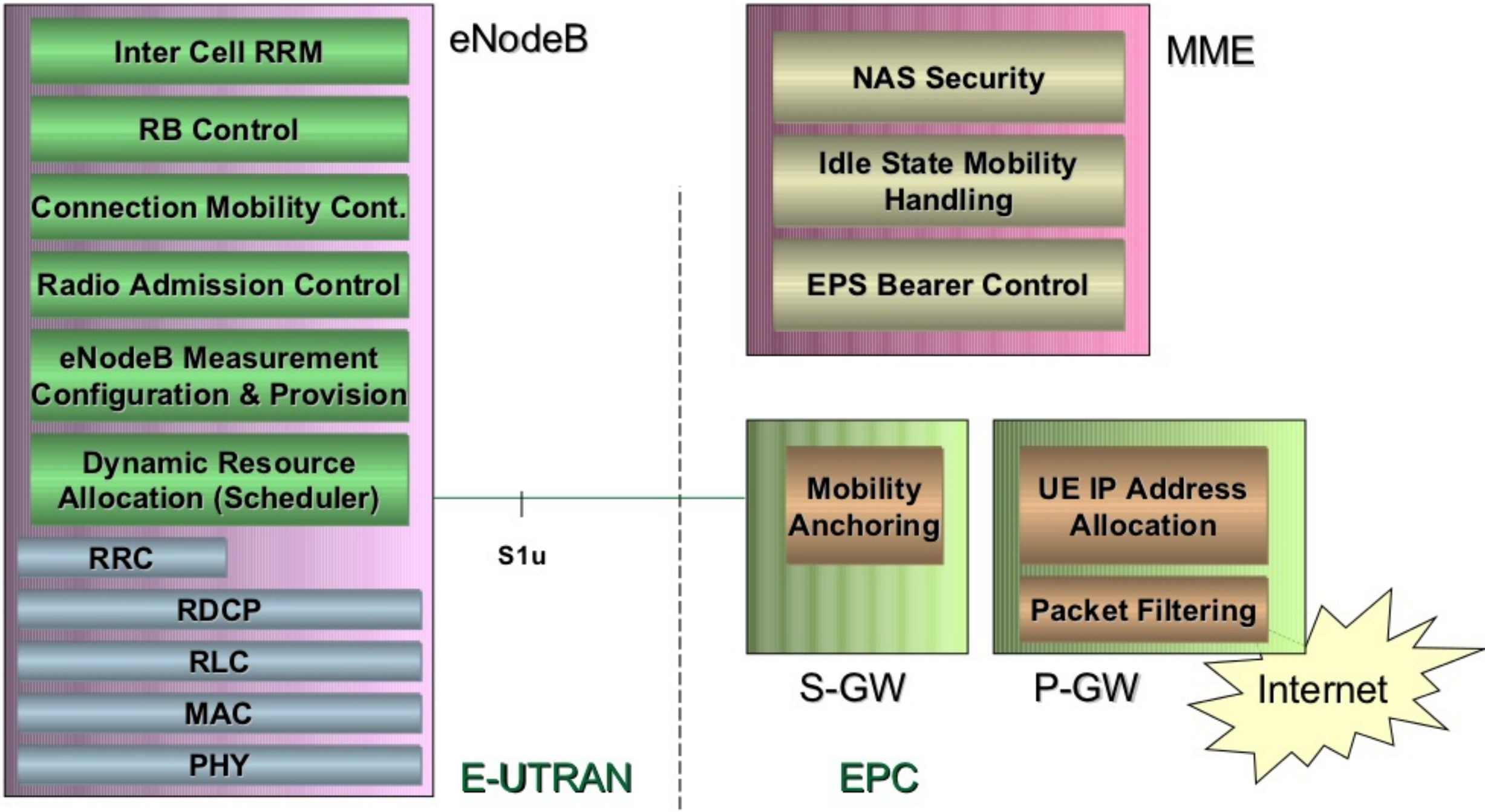


LTE Architecture Overview

- LTE network is comprised of the Core (EPC) and the access network (E-UTRAN). Interfaces are standardized to allow multi-vendor interoperability.



E-UTRAN vs EPC



The Core Network

- **MME**: It is the control node that processes the signaling between UE and the Core Network (CN). The protocols running between the UE and the CN are known as the *Non-Access Startum (NAS)* Protocols.
- **S-GW**: Local mobility anchor for data bearers when UE moves between eNodeBs. It retains the information about the bearers when UE is in idle state and temporarily buffers downlink data. It collects charging information and legal interception.
- **P-GW**: IP address allocation. QoS enforcement. Flow-based charging. Filtering downlink IP packets into different QoS bearers.
- **HSS**: Contains user subscription data such as subscribed QoS profile, subscribed APNs. It keeps track of MME identity to which the user is attached to. It also generates authentication and security keys.
- **PCRF**: Responsible for policy control decision-making, as well as controlling the flow-based charging functionalities in Policy Control Enforcement Function (PCEF) which resides in the P-GW.

Non Access Startum (NAS) Procedures

- Non Access Startum are the protocols and procedures that run between UE and core network (MME) transparently through eNodeB.
- MME maintains a UE context, assigned a unique SAE-Temporary Mobile Subscriber Identity (S-TMSI).

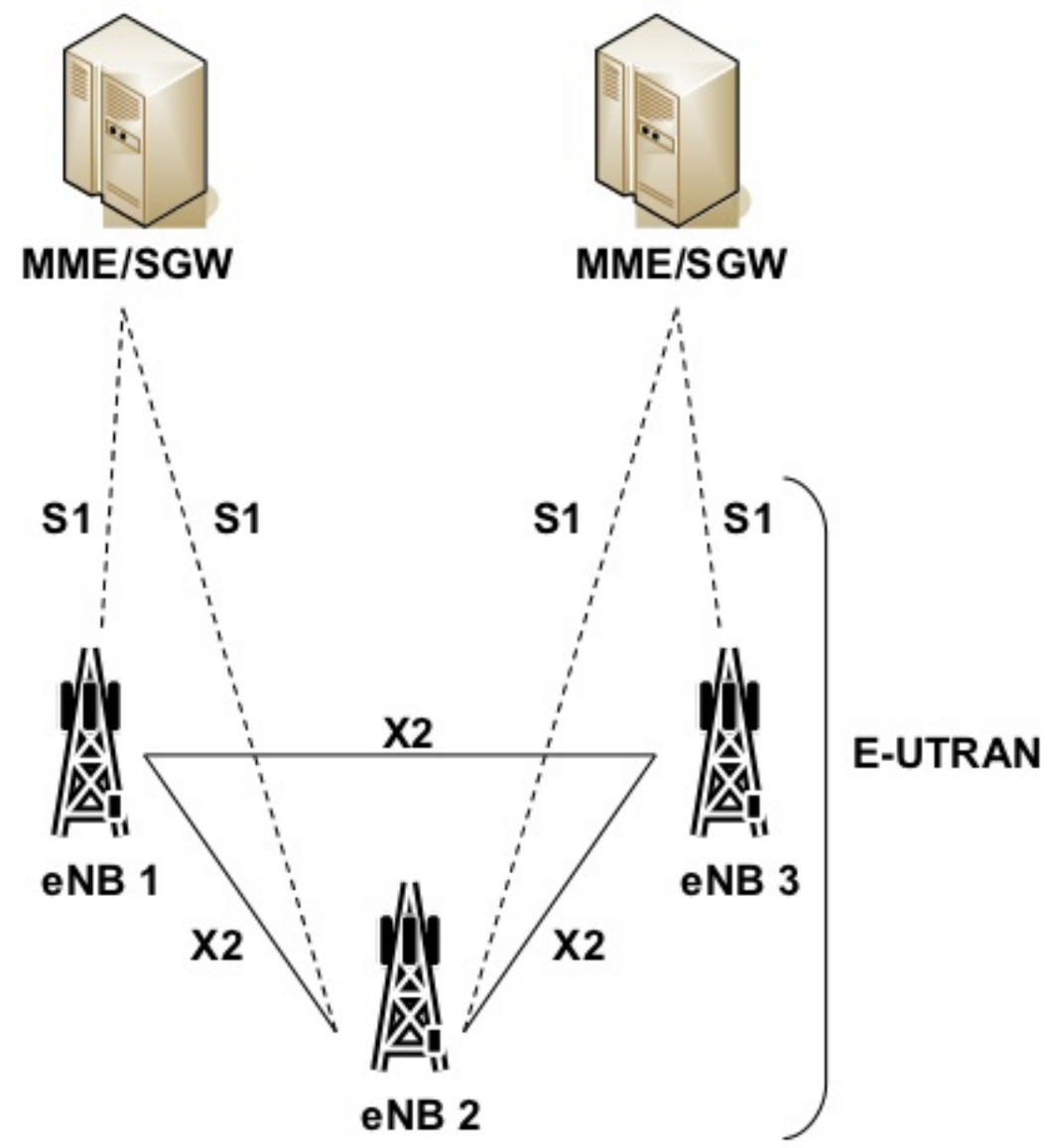
- UE context moves from MME to eNodeB when there is a need to deliver downlink data, moving UE from ECM-Idle to ECM-Connected by means of UE paging. During periods of UE inactivity, UE context moves back from eNodeB to MME, moving UE back to ECM-Idle.

The Access Network

- E-UTRAN simply consists of eNodeBs, there is no centralized controller, hence E-UTRAN architecture is said to be flat, reducing latency and improving efficiency.
- eNodeBs are inter-connected by means of X2 Interface, and to the EPC by means of S1 Interface. S1-U to S-GW and S1-MME to MME.
- The protocols which run between the eNodeB and the UE are known as the Access Startum (AS) Protocols.

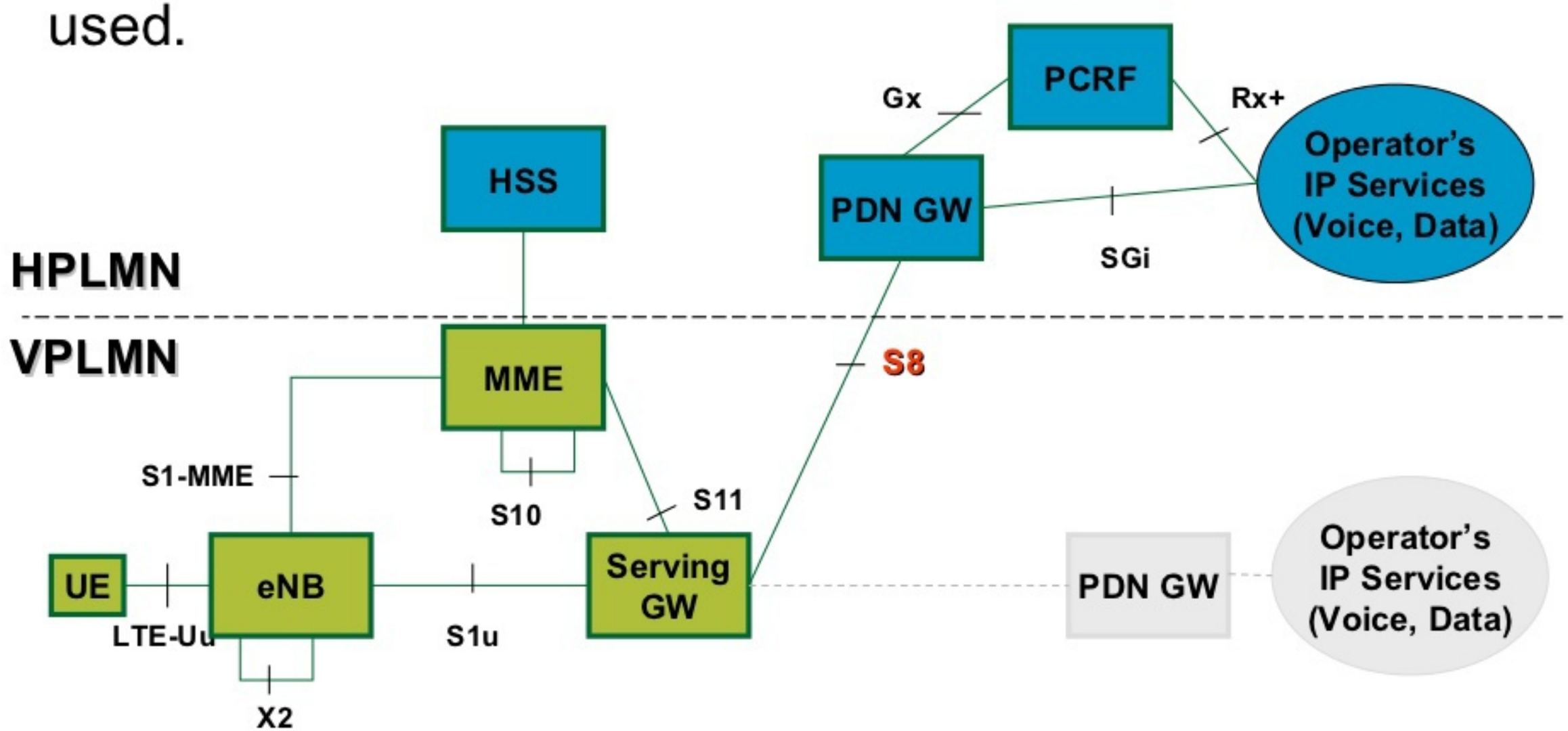
The Access Network

- E-UTRAN Functions:
  - Radio Resource Management:
    - Radio bearer control.
    - Radio admission control.
    - Radio mobility control.
    - DL/UL resources Scheduling.
  - Header Compression.
  - Security and Encryption.
  - Connectivity to the EPC
    - Signaling to MME.
    - Bearer path to S-GW.



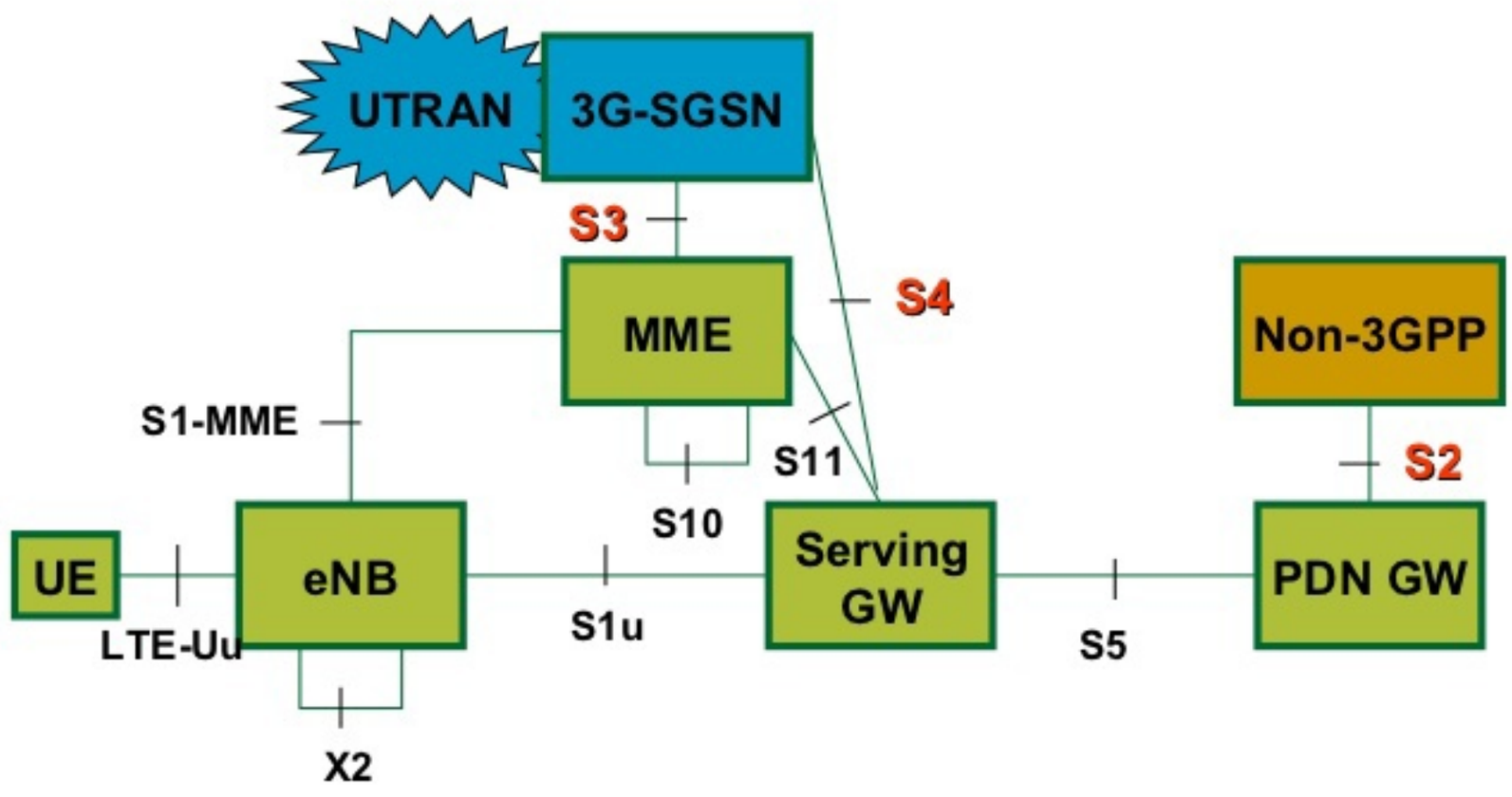
Roaming Architecture

- A roaming user is connected to E-UTRAN, MME, and S-GW of the visited LTE network. However, LTE/SAE allows the P-GW of either the visited or the home network to be used.



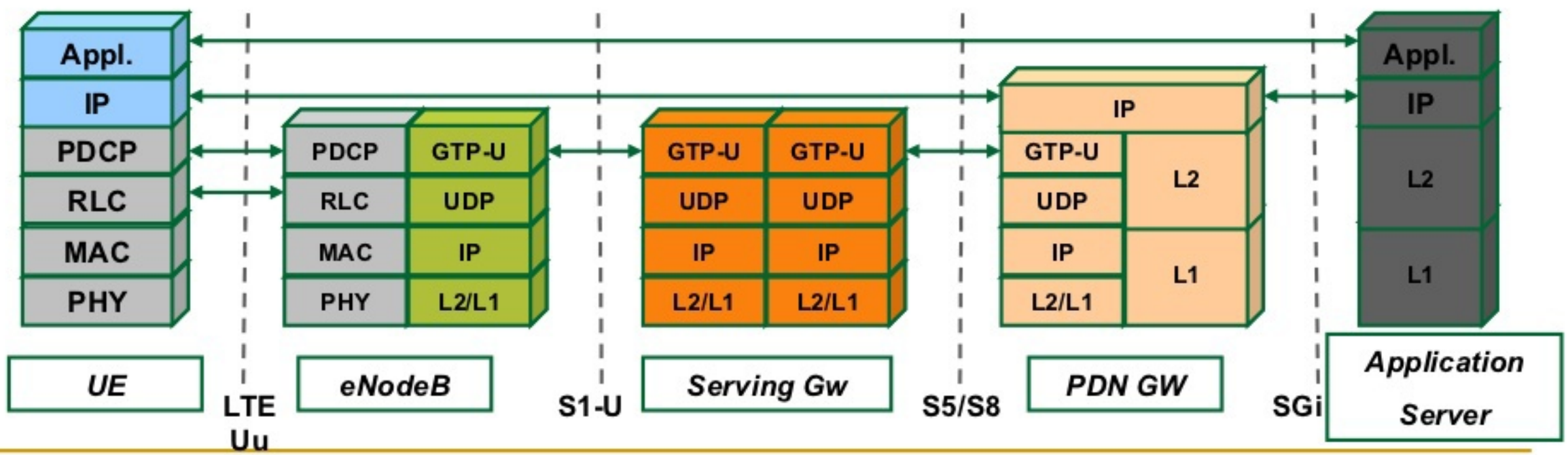
Inter-Working with other Networks

- EPS supports inter-working and mobility (handover) with other Radio Access Technologies (RATs), notably GSM, UMTS and WiMAX. S-GW acts as the mobility anchor for inter-working with other 3GPP technologies such as GSM/UMTS, while P-GW serves as an anchor allowing seamless mobility to non-3GPP netowrks.



Protocol Architecture: User Plane

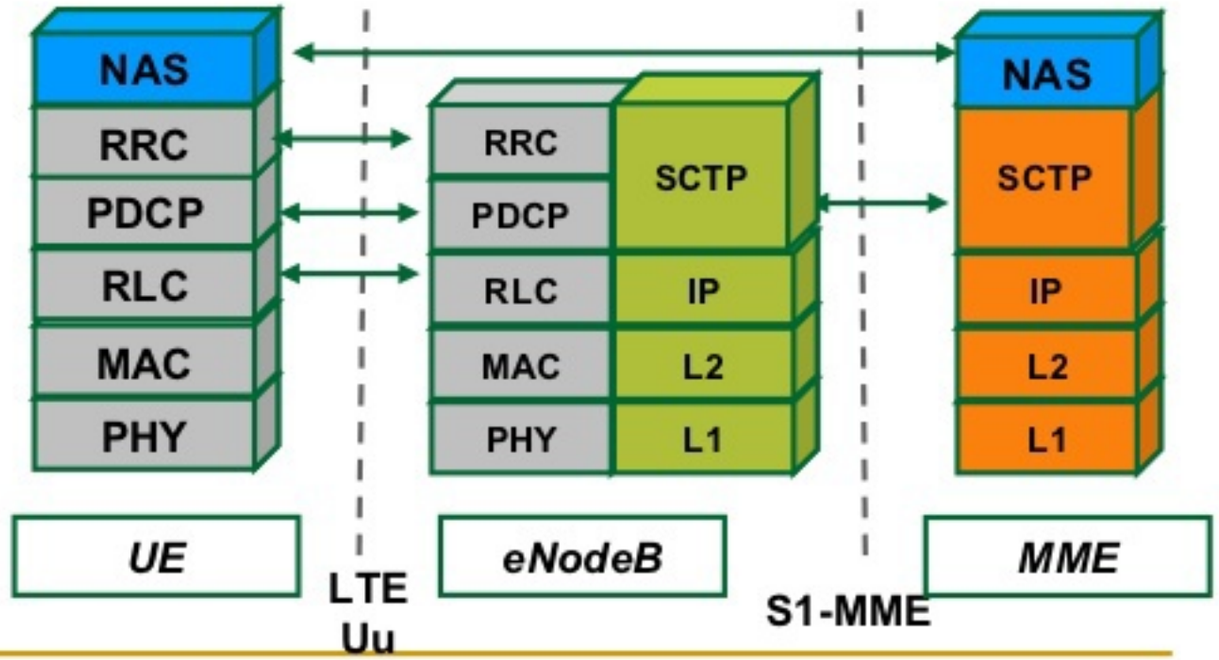
- IP packets from UE are encapsulated in GPRS Tunneling Protocol (GTP) between eNB and P-GW over S1 and S5/S8 interfaces.
- E-UTRAN user plane protocol stack is shown greyed below.



Protocol Architecture: Control Plane

- There is no header compression function for control plane. Header compression is used in user plane only.
- The access startum protocols are shown in grey.
- The non-access startum protocols are shown in blue.

- The RRC protocol is the main controlling function in the access startum, being responsible for establishing the radio bearers and configuring lower layers

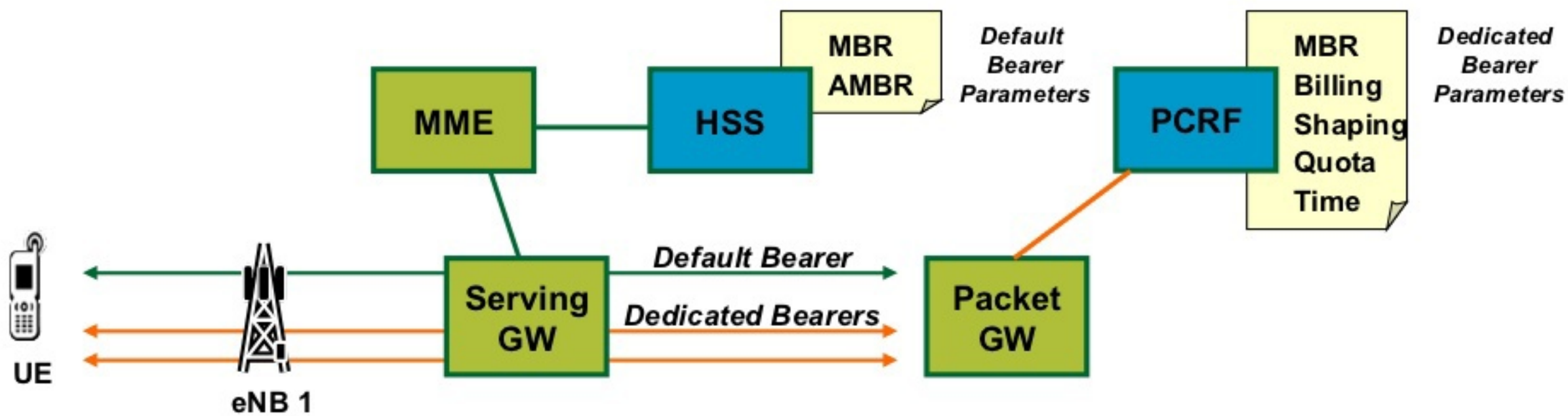


Quality of Service

- In order to support multiple QoS requirements, different bearers are set up within EPS, each associated with a QoS.
- Bearers are classified into:
  - **Minimum Guaranteed Bit Rate (GBR) bearers**: used for applications such as VOIP. These bearers have a permanently dedicated transmission resources. Bit rates higher than GBR may be allowed if resources are available, where a Maximum Bit Rate (MBR) sets an upper limit on the bit rate.
  - **Non-GBR bearers**: don't guarantee any particular bit rate. Used for web browsing or FTP.

Quality of Service

- UE default bearer is always non-GBR bearer.
- Default bearer parameters (i.e. maximum bit rate) are saved in HSS. Dedicated bearer parameters are dynamically populated in PCRF.



Quality of Service

- Each EPS bearer is associated QoS Identifier (QCI) and an Allocation and Retention Priority (ARP).
- Nine QCIs have been standardized to ensure same QoS treatment regardless of multi-vendors in LTE network.
- ARP is used for call admission control, i.e., to decide whether or not the requested bearer should be established in case of radio congestion. Once successfully established, ARP has no impact on the bearer packet forwarding treatment.
- QCI decides how the scheduler in eNodeB handles packets. Acknowledged mode (AM) is used for bearers with low packet loss rate, while Unacknowledged mode is used for delay sensitive data.

QCI = GBR/ Non-GBR + Priority + Packet Delay + Packet Loss

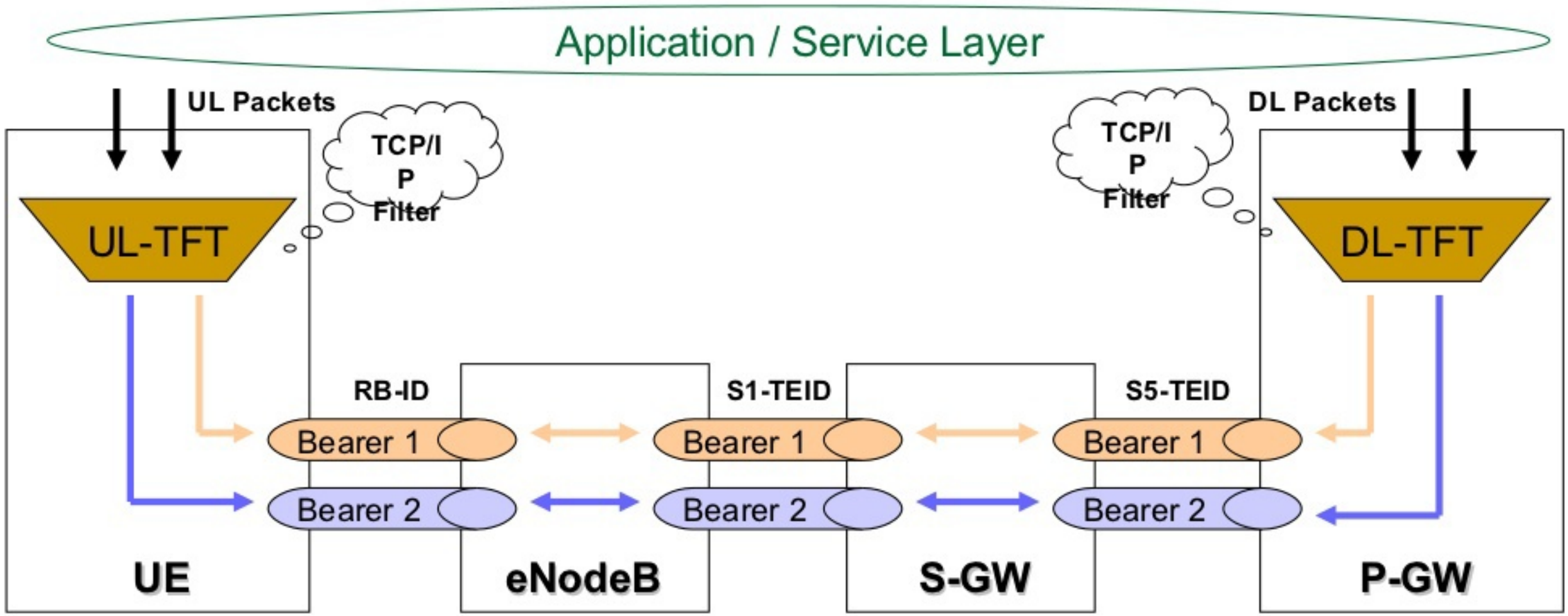
Standardized QCI

QCI	Resource Type	Priority	Packet Delay (ms)	Packet Loss Rate	Example Service
1	GBR	2	100	10^{-2}	Conversational Voice
2	GBR	4	150	10^{-3}	Conversational Video
3	GBR	5	300	10^{-6}	Buffered Streaming
4	GBR	3	50	10^{-3}	Real Time Gaming
5	Non-GBR	1	100	10^{-6}	IMS Signaling
6	Non-GBR	7	100	10^{-3}	Interactive Gaming
7	Non-GBR	6	300	10^{-6}	Video Buffered Streaming
8	Non-GBR	8	300	10^{-6}	WWW, FTP, p2p
9	Non-GBR	9	300	10^{-6}	Progressive Video

EPS bearer mapping

- As the packet transports LTE interfaces, bearers mapping is performed to guarantee end-to-end QoS treatment for the packet flow.
- Traffic Flow Templates (TFT) are used to filter packets into different bearers at the end points of EPS, i.e., at UE or P-GW. TFTs use IP header information such as source and destination IP and TCP port.
- Uplink TFT in UE filters IP packets to EPS bearers in the uplink direction. Downlink TFT in P-GW is a similar set of downlink packets filters.

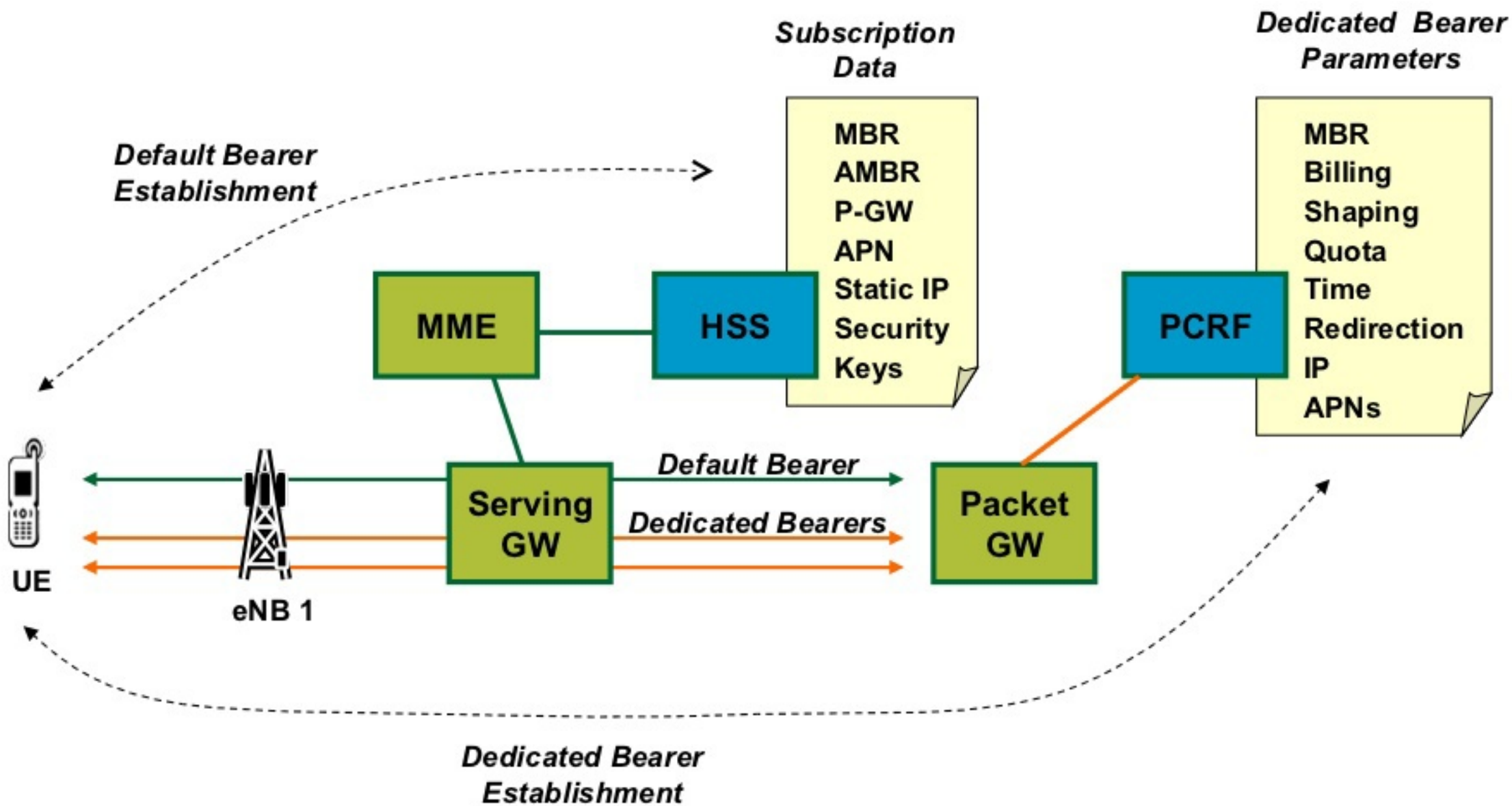
EPS bearer mapping



Default Bearer Establishment

- When UE attaches to the network, the UE is assigned IP address and one default bearer, providing an always-on IP connectivity to PDN.
- The initial bearer QoS is assigned by the MME, based on subscription data retrieved from HSS.
- Dedicated bearers can be establishment any time during the call, and it can either be GBR or non-GBR. The default bearer is always non-GBR.
- Dedicated bearer QoS are received by P-GW from the PCRF and forwarded to S-GW.

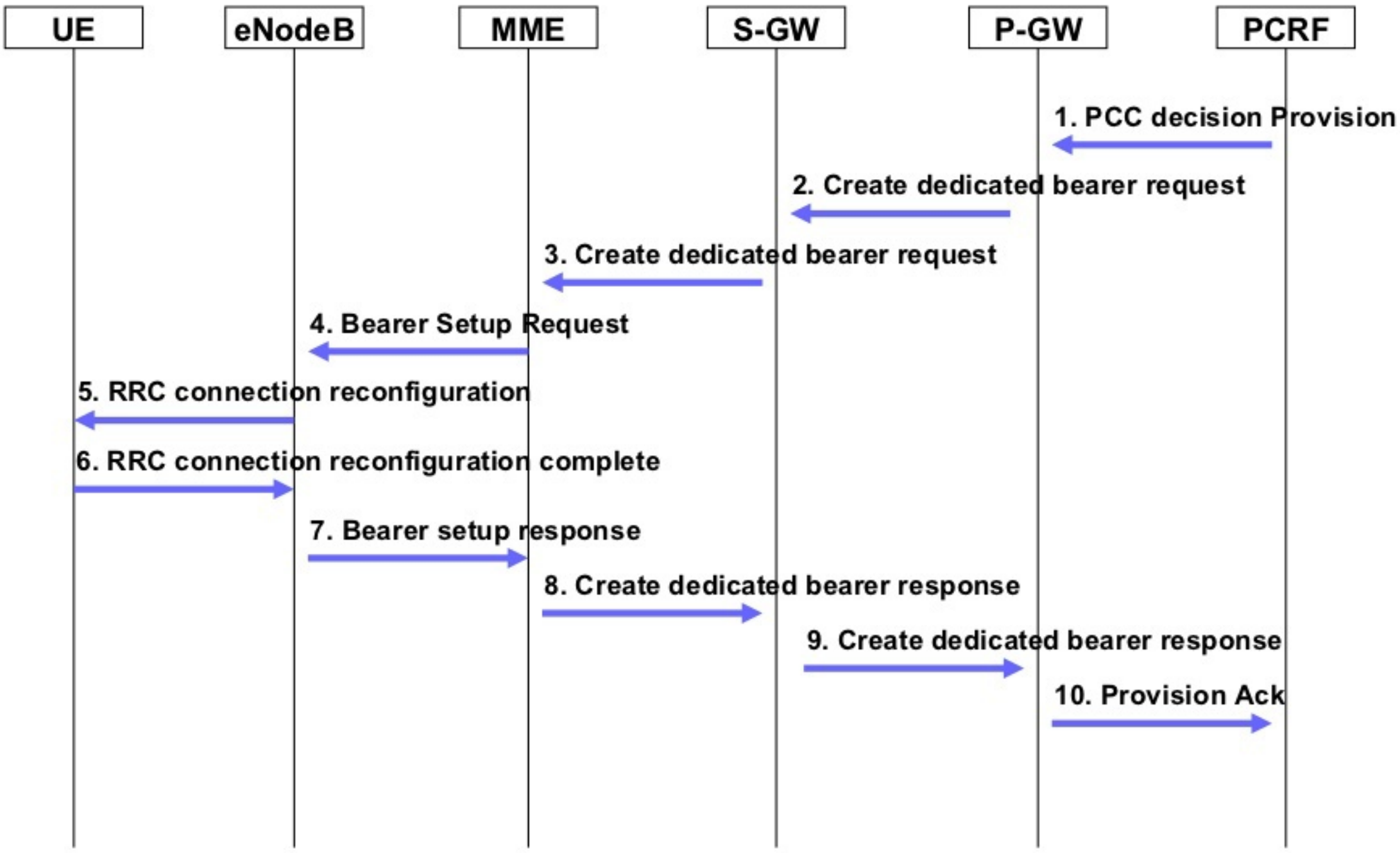
Default Bearer Establishment



Bearer Establishment Procedure

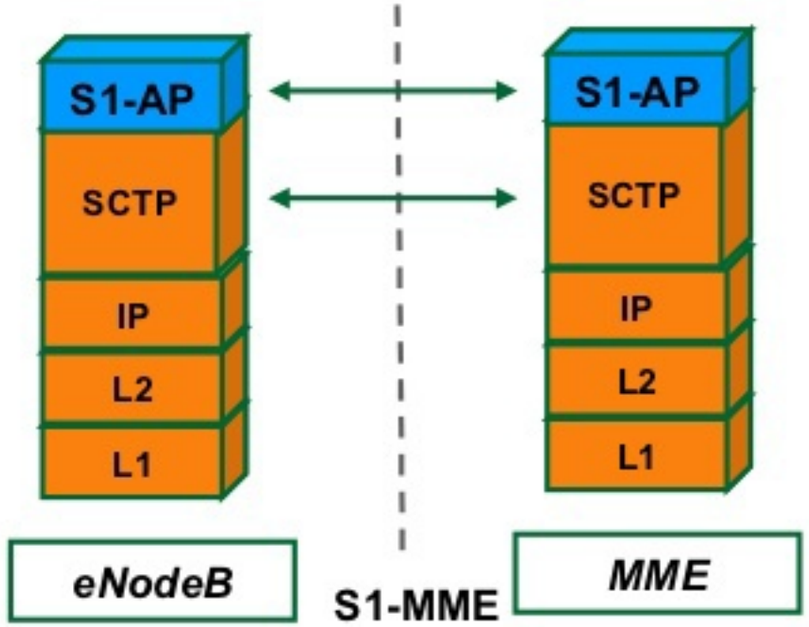
1. PCRF indicates the required QoS for the bearer in “PCC Decision Provision” message.
2. P-GW sends “Create Dedicated Bearer Request” including QoS and UL TFT to be used in UE to the S-GW.
3. S-GW adds S1-bearerID to the message and send it to the MME.
4. MME builds session management configuration including UL TFT and EPS bearerID and send it to eNodeB. The NAS information is sent transparently by eNodeB to the UE.
5. eNodeB uses bearer QoS for admission control and maps EPS bearer QoS to radio bearer QoS.

Bearer Establishment Procedure



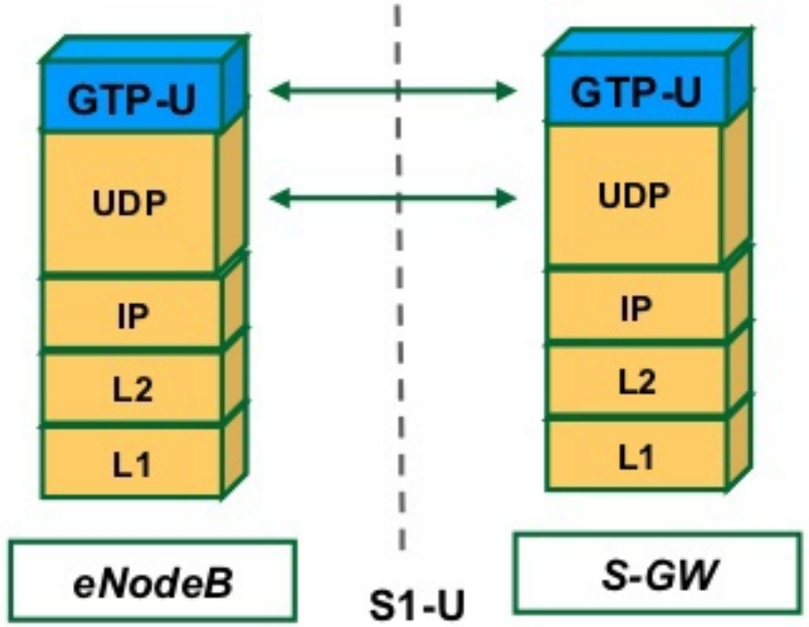
The S1 Interface: Control Plane

- S1-MME is based on a full IP/SCTP stack with no dependency on legacy SS7.
- SCTP is well known for the reliability of data delivery for signaling messages, and the handling of multi-streams to implement transport network redundancy.



The S1 Interface: User Plane

- S1-U is based on the GTP/UDP/IP stack which is already well known from UMTS networks.
- GTP-User plane (GTP-U) is used for its inherent facility to identify tunnels and to facilitate intra-3GPP mobility.
- A transport bearer is identified by the GTP tunnel endpoints (TEID) and the IP address.

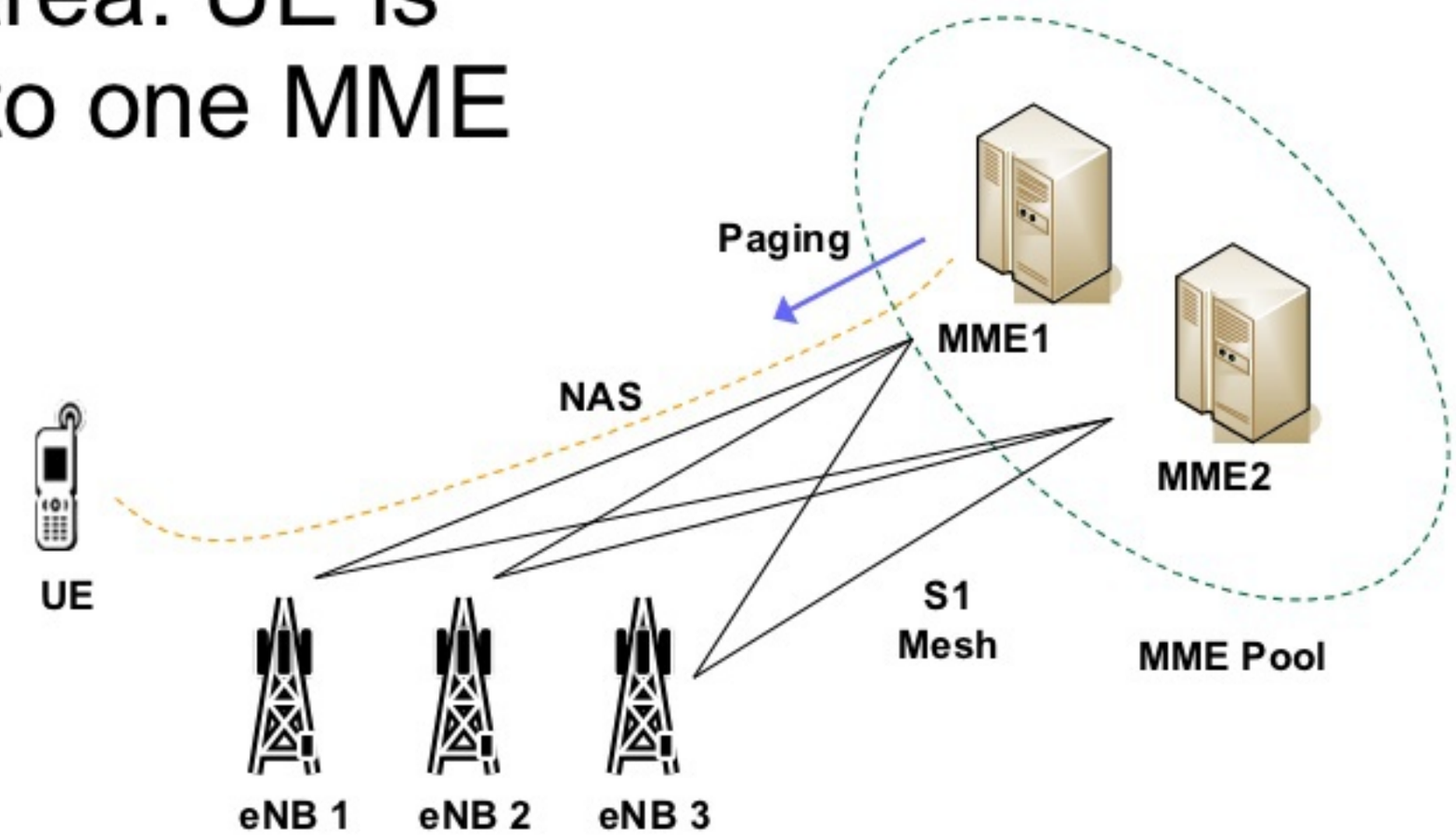


S1 Interface Procedures

- **S1 Initiation**: eNodeB initiates an S1 interface towards each MME in the pool area, providing S1 redundancy.
- **Context Management over S1**: each UE is associated to one particular MME in MME pool area. Whenever the UE becomes active, the MME provides the UE context to the eNodeB.
- **Bearer Management over S1**: MME provides eNodeB with IP address of S-GW (termination point for UE bearer), QoS and TEID of UE bearer.

S1 Topology

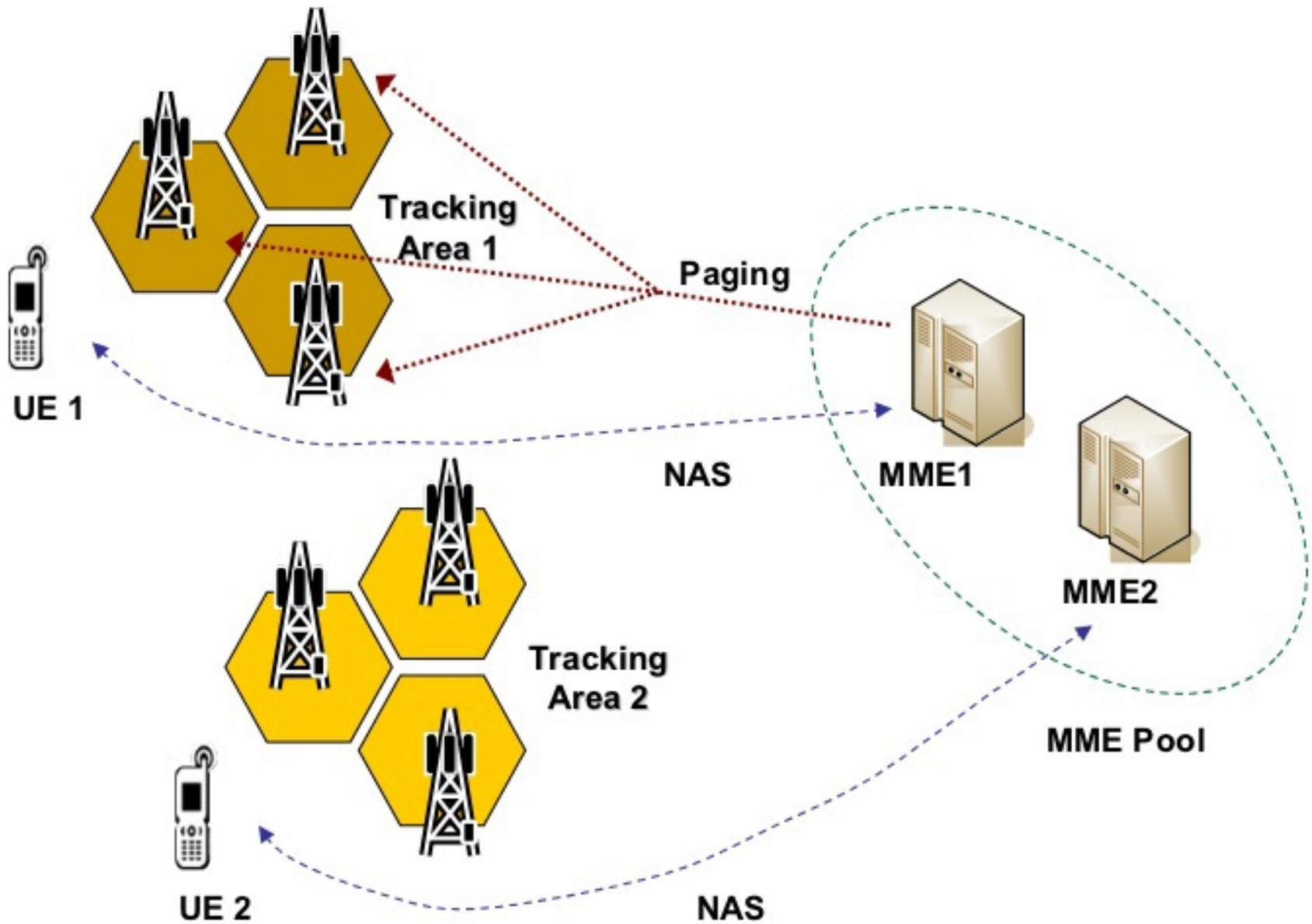
- eNodeBs maintains S1 interface with all MMEs in MME pool area. UE is associated to one MME only.



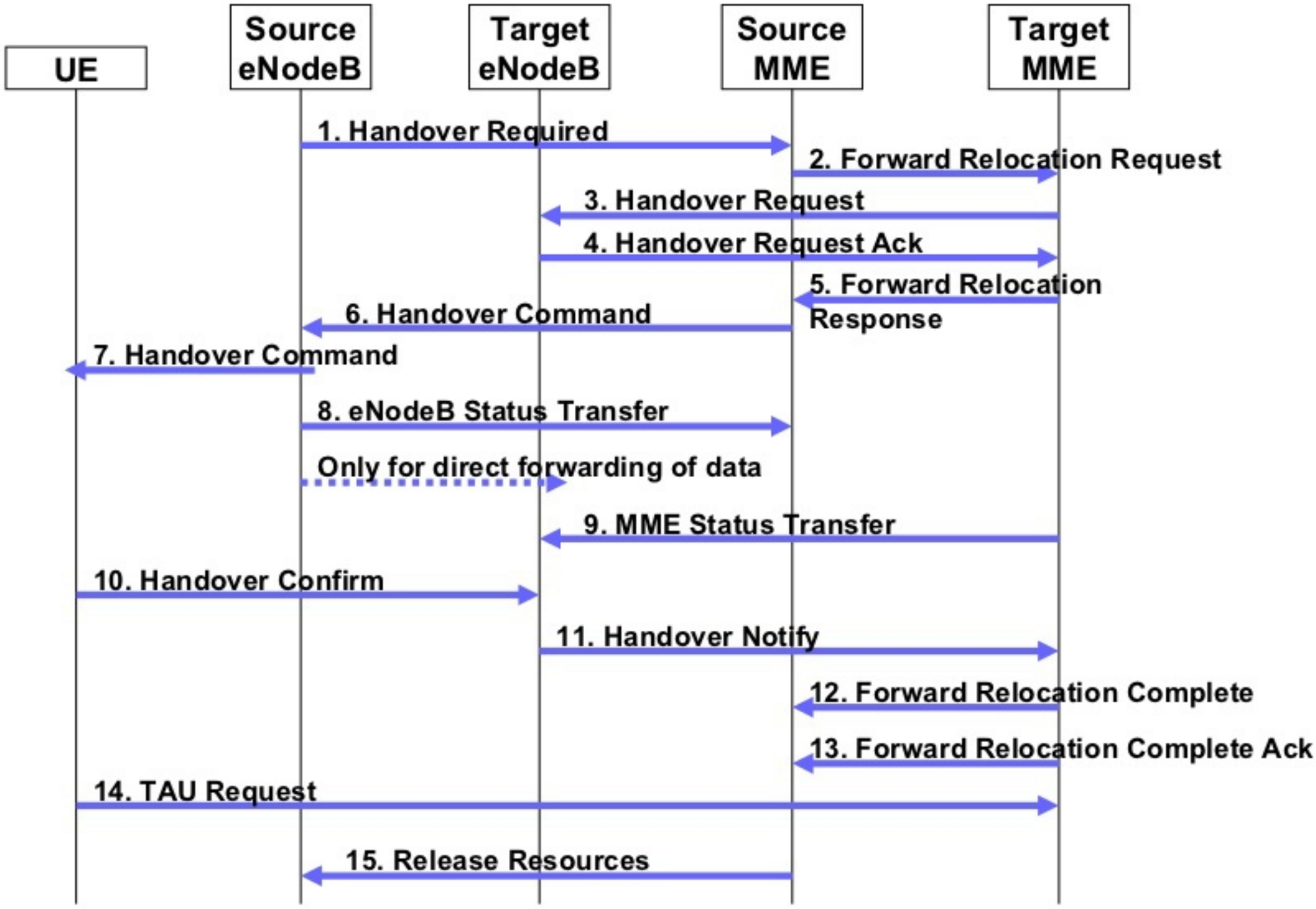
S1 Interface Procedures

- **Paging over S1**: Upon reception of downlink data, MME sends paging request for a particular UE to all eNodeBs in the tracking area where UE is located.
- **Mobility over S1**: when there is no X2 interface between eNodeBs, or if handover is configured to be via S1 interface, then S1-handover will be triggered.
- **Load Management over S1**: UEs are evenly distributed among MMEs in MME-pool.

S1 Interface Procedures

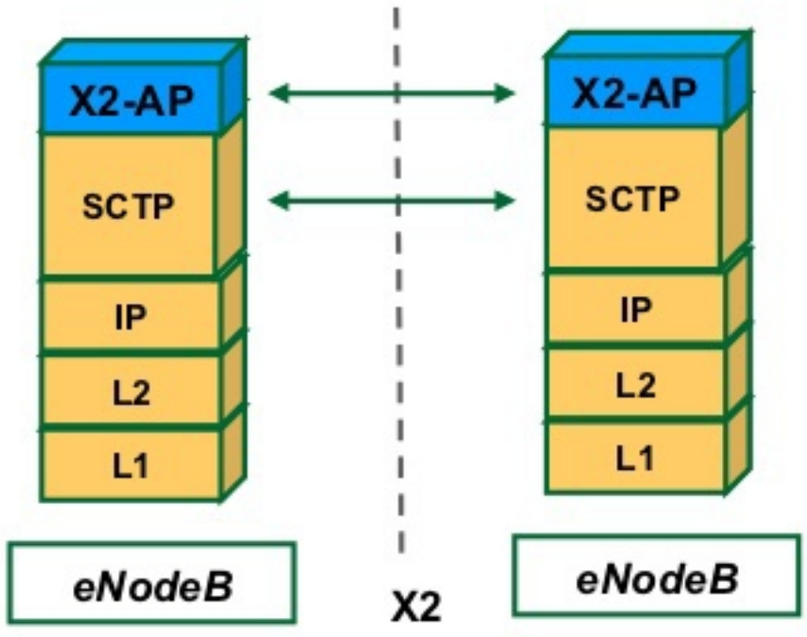


S1-based Handover



X2 Interface

- X2 is used to inter-connect eNodeBs. The control plane and user plane stack over X2 interface is the same as S1-MME.
- X2 interface may be established between one eNodeB and some of its neighbors. However, a full mesh is not mandated in E-UTRAN network.
- X2 interface is used for
  - Mobility.
  - Load and interference management.

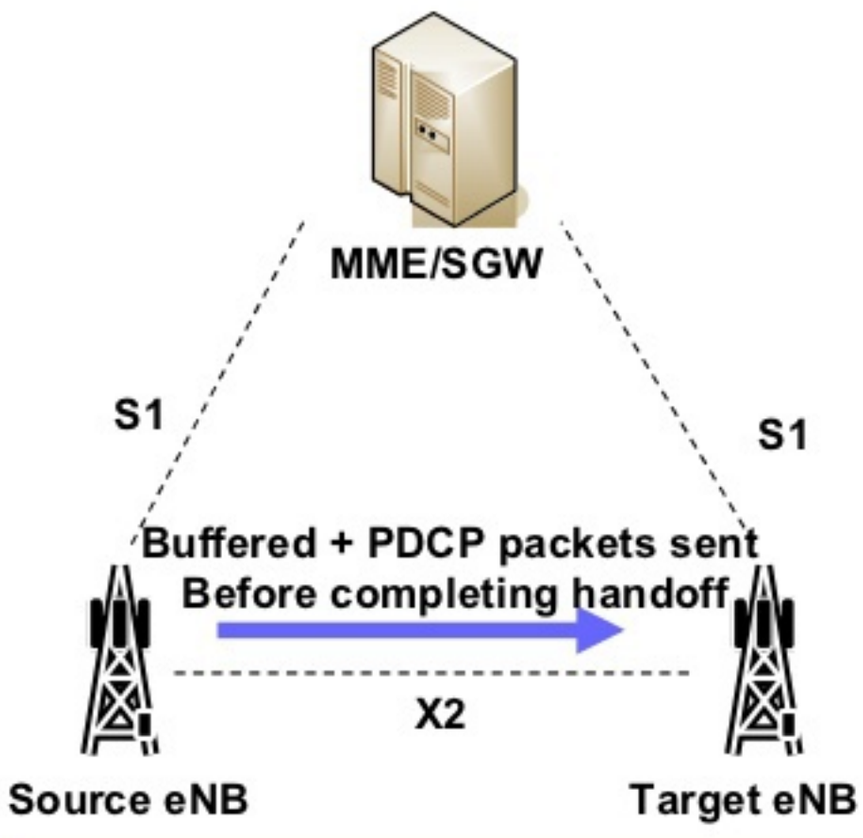


X2 Interface Procedures

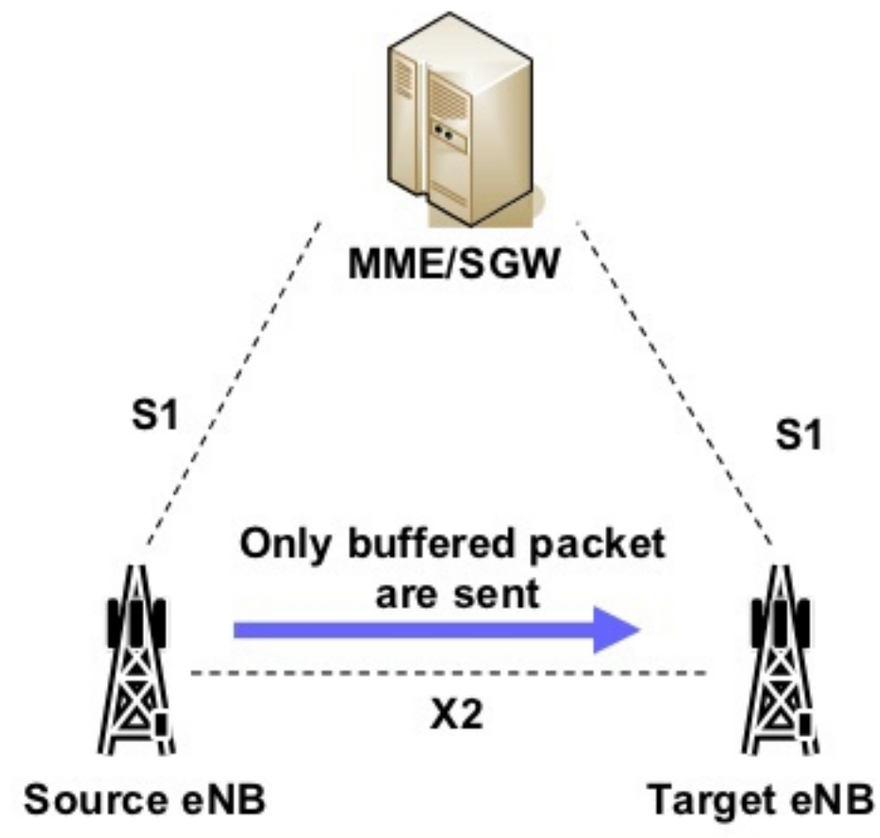
- Mobility over X2:
  - Handover via X2 is triggered by default unless there is no X2 interface or eNodeB is configured to use S1-handover instead.
  - Handover is directly performed between two eNodeBs, MME is only informed at the end of the handover.
  - Seamless handover: Packets scheduled in PDCP layer in source eNodeB layer will be lost during handoff.
  - Lossless handover: Packets scheduled in PDCP layer are sent over X2 interface during handoff.

Seamless vs Lossless Handover

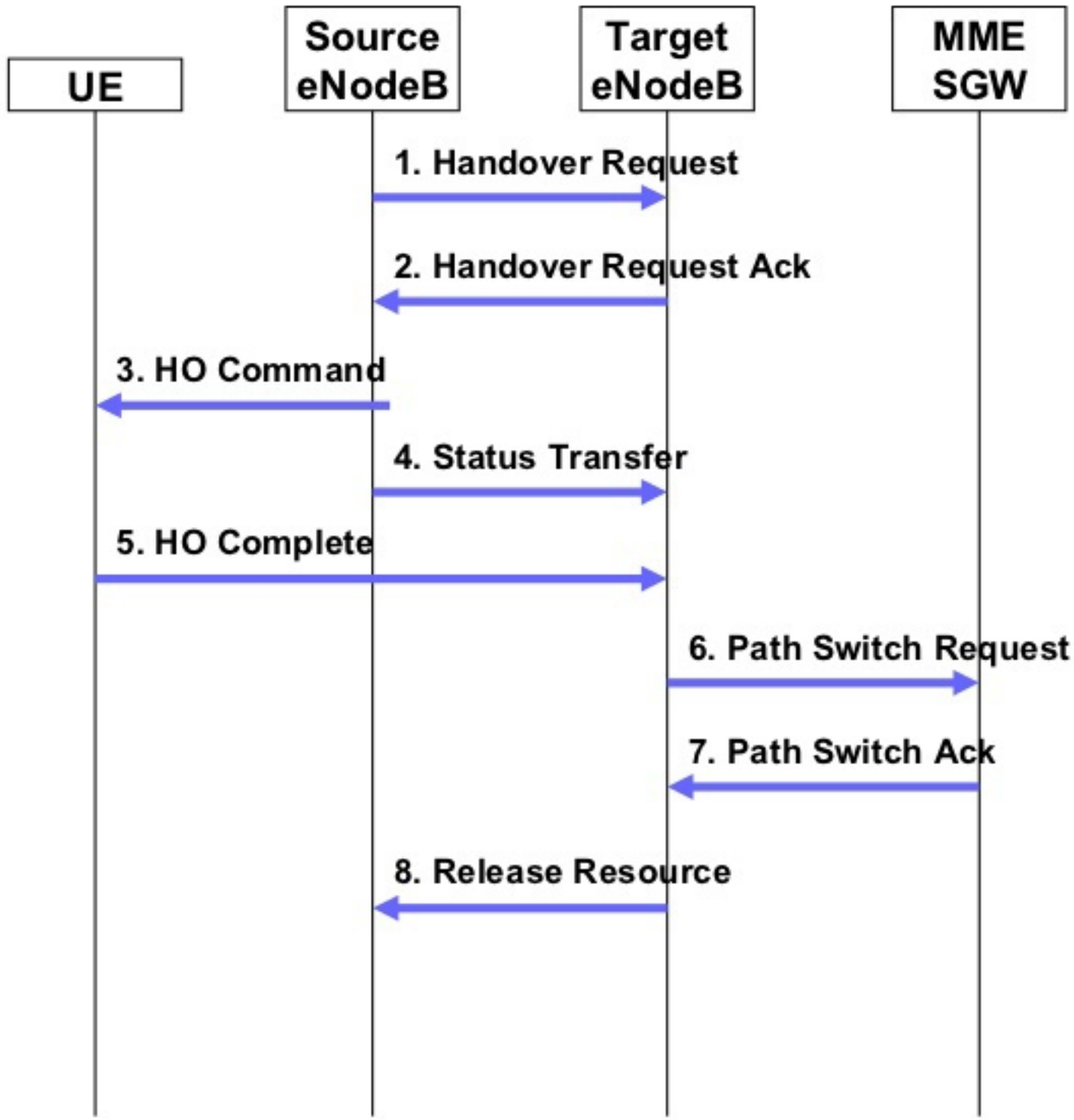
- Lossless Handoff: buffered packets as well as packets scheduled for transmission in PDCP layer are sent to target eNB before completing handover



- Seamless Handoff: only buffered packets are sent to target eNB before completing handover. Packets scheduled in PDCP layer are lost, and will be retransmitted in upper layers



X2-based Handover Procedure



X2 Interface Procedures

- Load and Interface Management over X2:
  - **Load Balancing**: a SON feature with the objective of load balancing traffic load between neighboring cells with the aim of improving overall system capacity.
  - **Interference Management**: another SON feature with the objective of reducing interference experienced by UEs by exchanging load information related to interference management between neighboring eNodeBs to improve overall system throughput.

Further Readings

- 3GPP Technical Specification 24.301, “Non-Access Startum Protocol for Evolved Packet System (EPS); Stage3 (Release 8)”, www.3gpp.org.
- 3GPP Technical Specification 33.401, “System Architecture Evolution (SAE): Security Architecture (Release 8)”, www.3gpp.org.
- 3GPP Technical Specification 29.060, “General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) (Release 8)”, www.3gpp.org.
- 3GPP Technical Specification 36.300, “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description (Release 8)”, www.3gpp.org.

LTE

3GPP Standard Perspective
Chapter 3 – Network Protocols

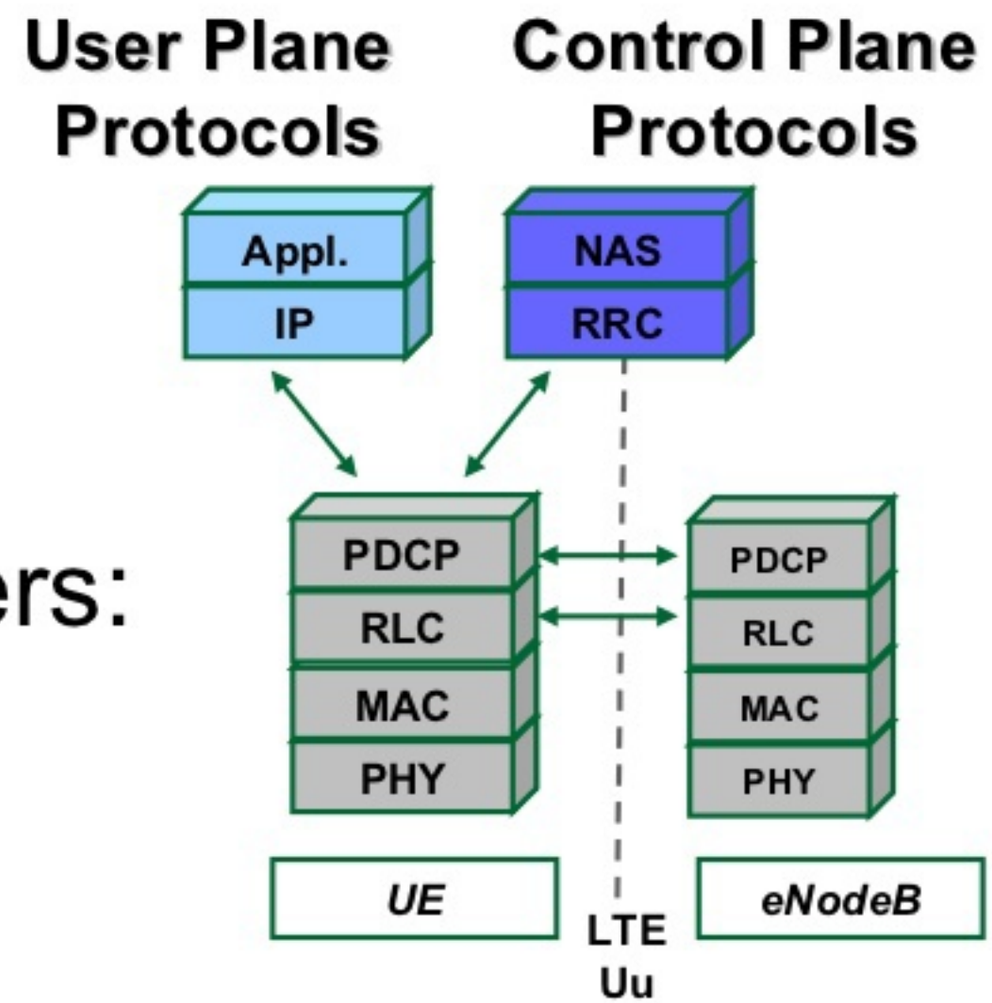
Muhannad Aulama

Contents of Chapter 3

- Introduction.
- Control Plane Protocols
- Radio Bearers .
- RRC Messages Mapping.
- System Information.
- Time Scheduling of System Information.
- Security Management.
- Ciphering vs Integrity Protection.
- Security Key Derivation.
- UE Connectivity Levels.
- Connection Establishment and Release.
- Radio Bearers Mapping.
- Mobility Control in RRC.
- Mobility in connected Mode.
- Measurements
- Radio Bearers Mapping.
- Mobility Control in RRC.
- Mobility in connected Mode.
- Measurements.
- Cell Selection.
- Cell Reselection.
- Paging.
- User Plane Protocols.
- PDCP Layer.
- PDCP Header Compression.
- PDCP PDU Format.
- RLC Layer.
- Unacknowledged Mode.
- UM HARQ Loss Detection & Reordering.
- Acknowledged Mode.
- Acknowledged Mode Retransmission.
- Media Access Control Layer.
- Logical Channels.
- Transport Channels.
- Multiplexing Between Logical Channels and Transport Channels.
- MAC Functions.
- MAC Resources Scheduling.
- MAC Functions.
- MAC Multiplexing and Prioritization.
- MAC Physical Channels.
- Further Readings.

Introduction

- LTE Network Protocols are either:
  - Control Plane Protocols
    - UE <-> eNodeB : RRC
    - UE <-> MME : NAS
  - User Plane Protocols
    - Applications IP data packets
- Control/User Common layers:
    - PDCP
    - RLC
    - MAC

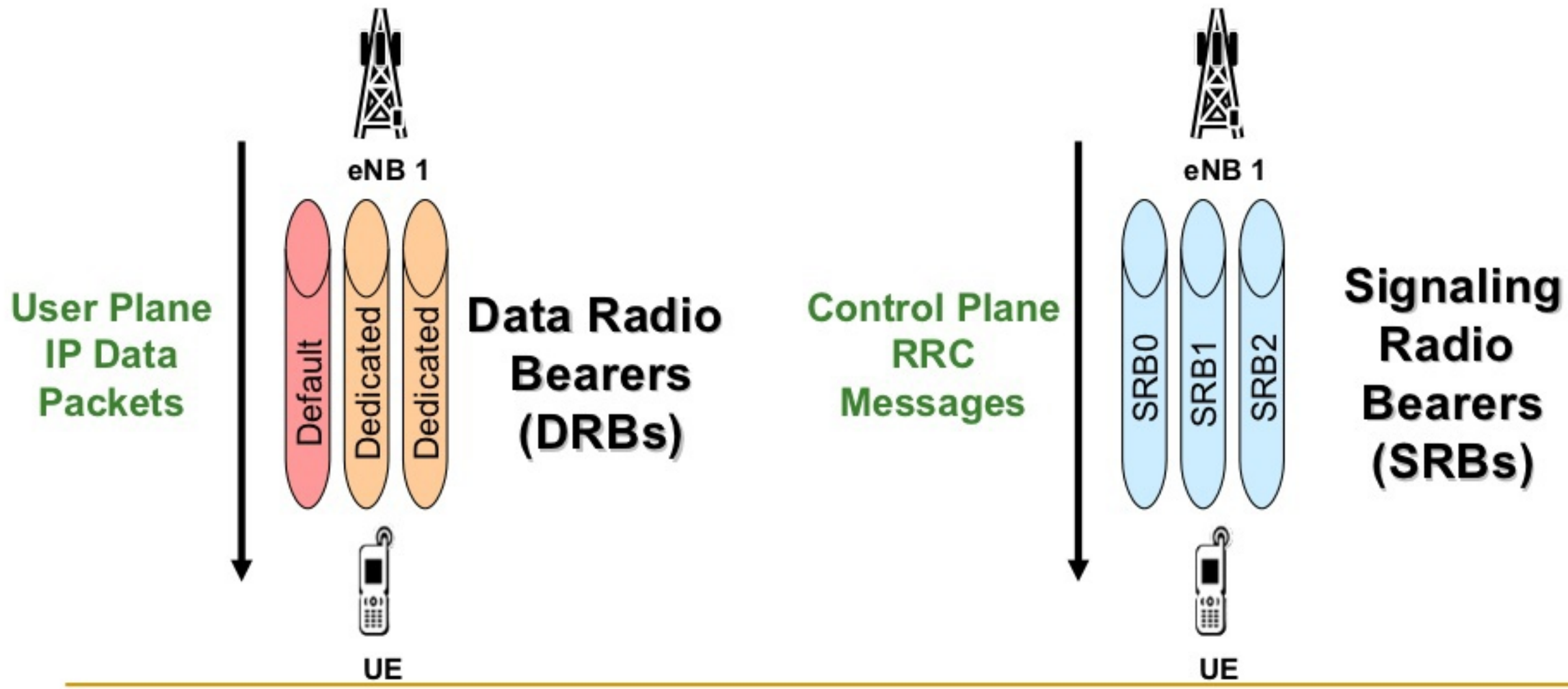


Control Plane Protocols

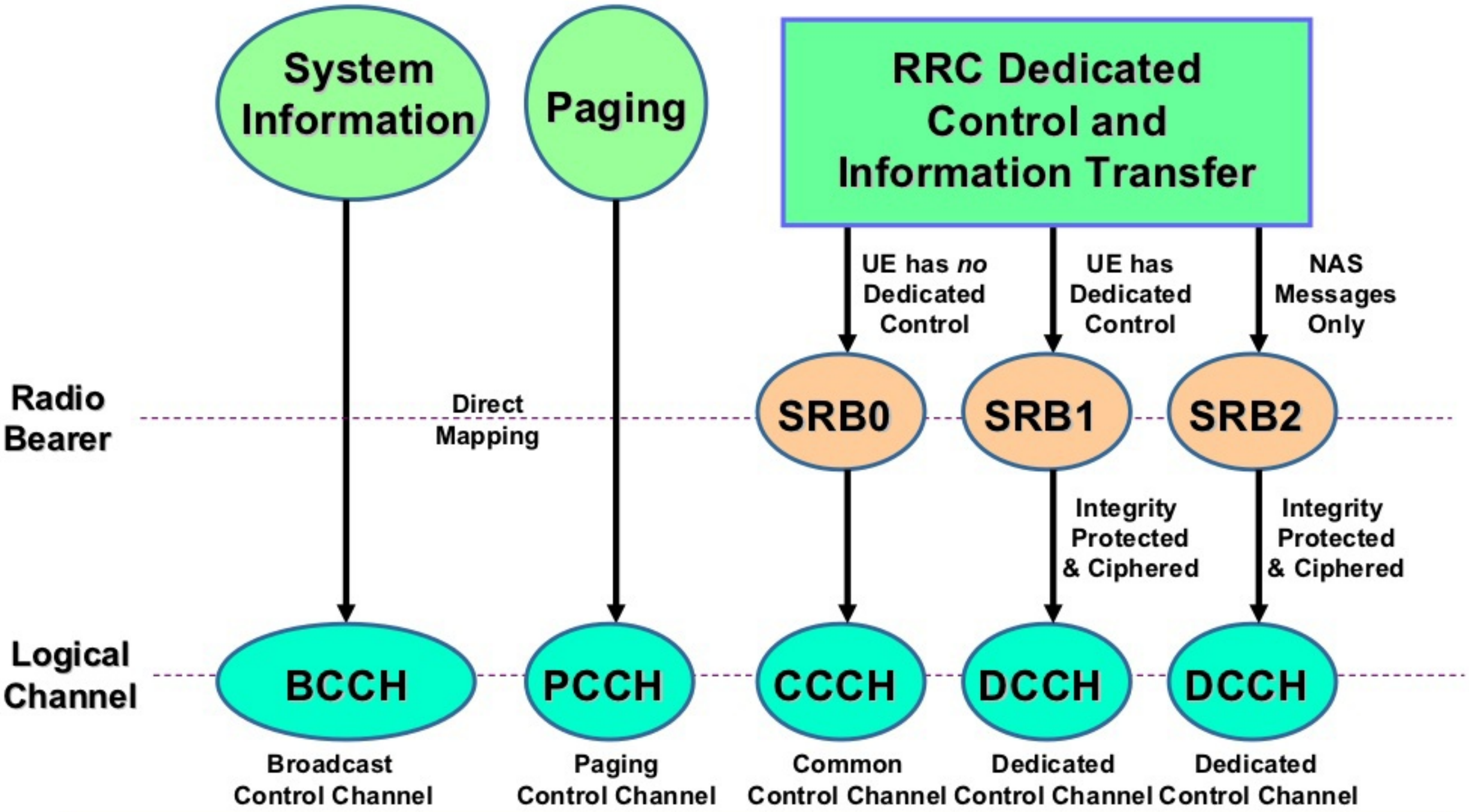
- Radio Resource Control (RRC) functions:
  - Broadcasting system Information.
  - RRC connection control.
    - Establishment/Release of radio bearers.
    - Paging and security activation.
    - Handover.
  - Measurement Reporting.
  - NAS transfer:
    - Transfer of dedicated NAS information to UE.

Radio Bearers

- All user and control plane packets are sent over Radio Bearers (RBs):



RRC Messages Mapping



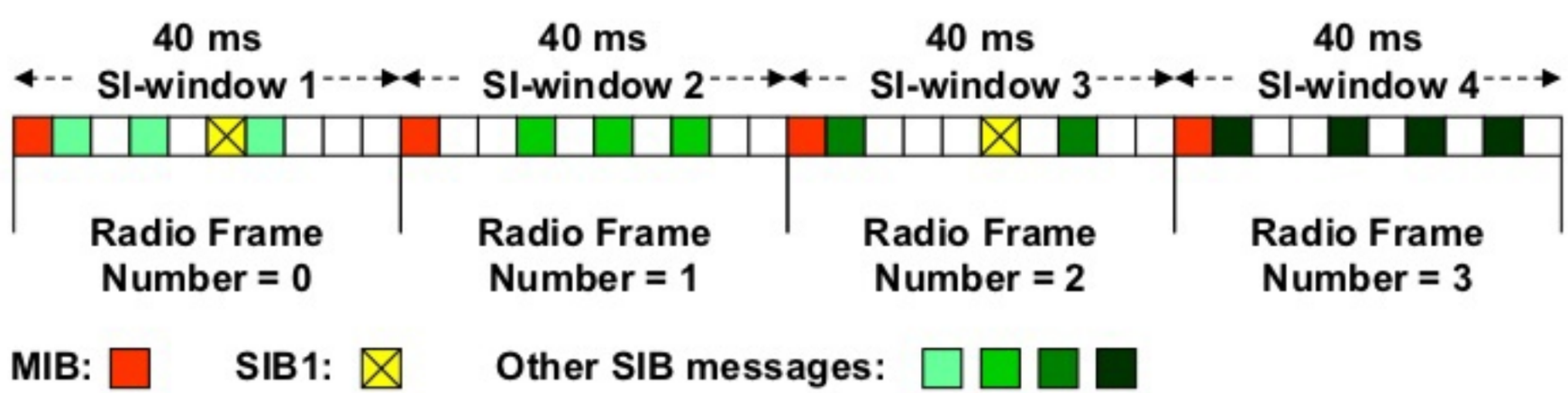
System Information

- System Information is structured in System Information Blocks (SIBs). SIB types are:

Messag	Current Release (Rel-6)	Perio	Applicability
MIB e	Most essential parameters	40 ms d	Idle & Connected
SIB1	Cell access related parameters	80 ms	Idle & Connected
SIB2	Common and shared channel configuration	160 ms	Idle & Connected
SIB3 & SIB4	SIB3: Common cell reselection information SIB4: Neighboring cell information	320 ms	Idle only
SIB5	Inter-frequency cell reselection information	640 ms	Idle only
SIB6 & SIB7	SIB6: UTRA cell reselection information SIB7: GERAN cell reselection information	640 ms	Idle only

Time Scheduling of System Information

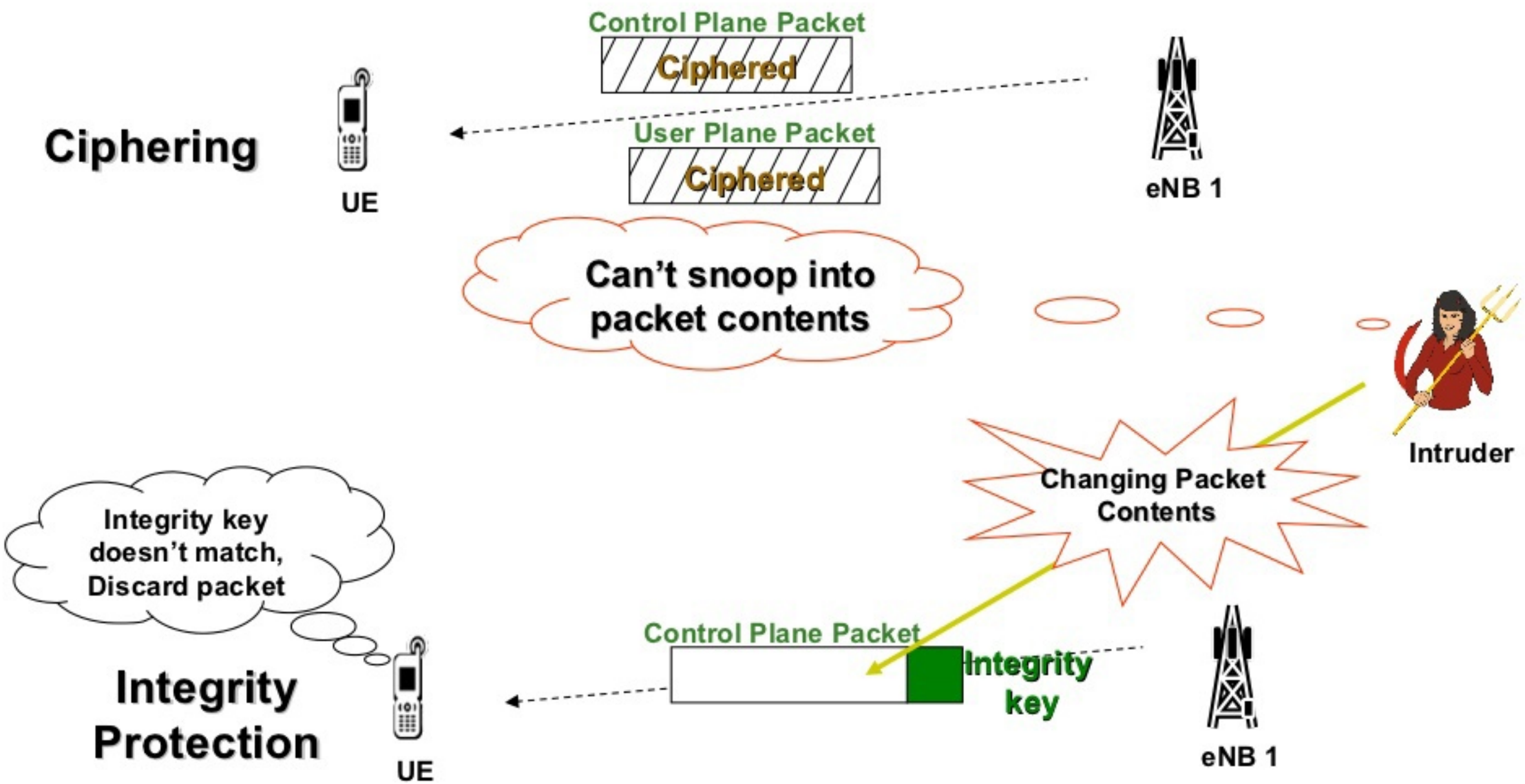
- Time scheduling of MIB and SIB1 is fixed; they have periodicities of 40 ms and 80 ms respectively.
- SIB1-7 periods are multiples of MIB period (40 ms), therefore MIB period is considered the System Information (SI) window for other SIBs.



Security Management

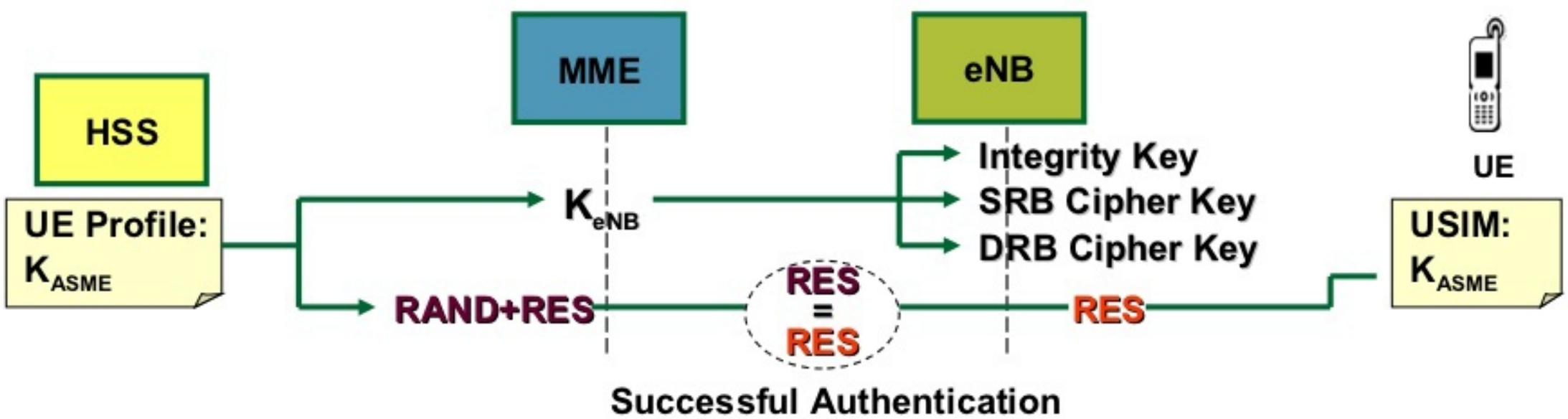
- Ciphering:
  - Both control plane (RRC) messages (SRBs 1 and 2), and user plane data (all DRBs) are ciphered.
- Integrity Protection:
  - Only for control plane (RRC) messages.
- Ciphering protects data streams from being received by a third party.
- Integrity protection allows the receiver to detect packet insertion or replacement.

Ciphering vs Integrity Protection



Security Key Derivation

- Access Startum base-key K_{eNB} is used to generate three further security keys:
  - Integrity protection key for RRC signaling (SRBs).
  - Ciphering key for RRC signaling (SRBs).
  - Ciphering key for user data (DRBs).



UE Connectivity Levels

- UE connectivity status is maintained in three levels:
  - EPS Mobility Management:
    - EMM-Deregistered: UE is deregistered in MME.
    - EMM-Registered: UE is registered in MME.
  - EPS Connectivity Management:
    - ECM-Idle: UE is not connected to the EPC.
    - ECM-Connected: UE is connected to EPC.
  - RRC Radio Level:
    - RRC-Idle: UE has no SRBs.
    - RRC-Connected: UE has SRBs and C-RNTI (*Cell Radio Network Temporary Identifier*).

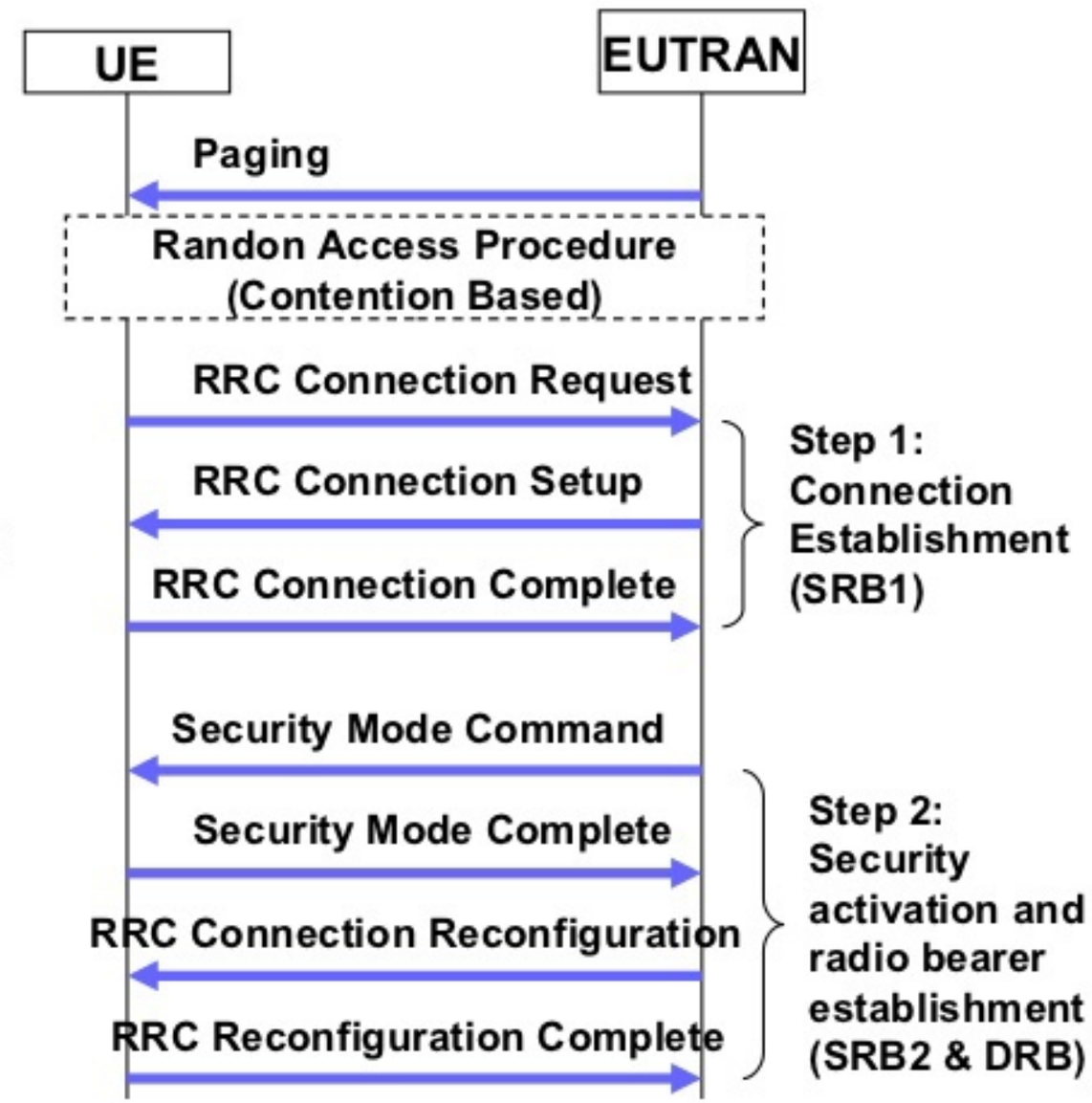
UE Connectivity Levels

- EMM and ECM connectivity levels are Non-Access Startum (NAS) states, while RRC connectivity level is Access Startum (AS).
- All three levels of UE connectivity are combined in the following possible combinations:

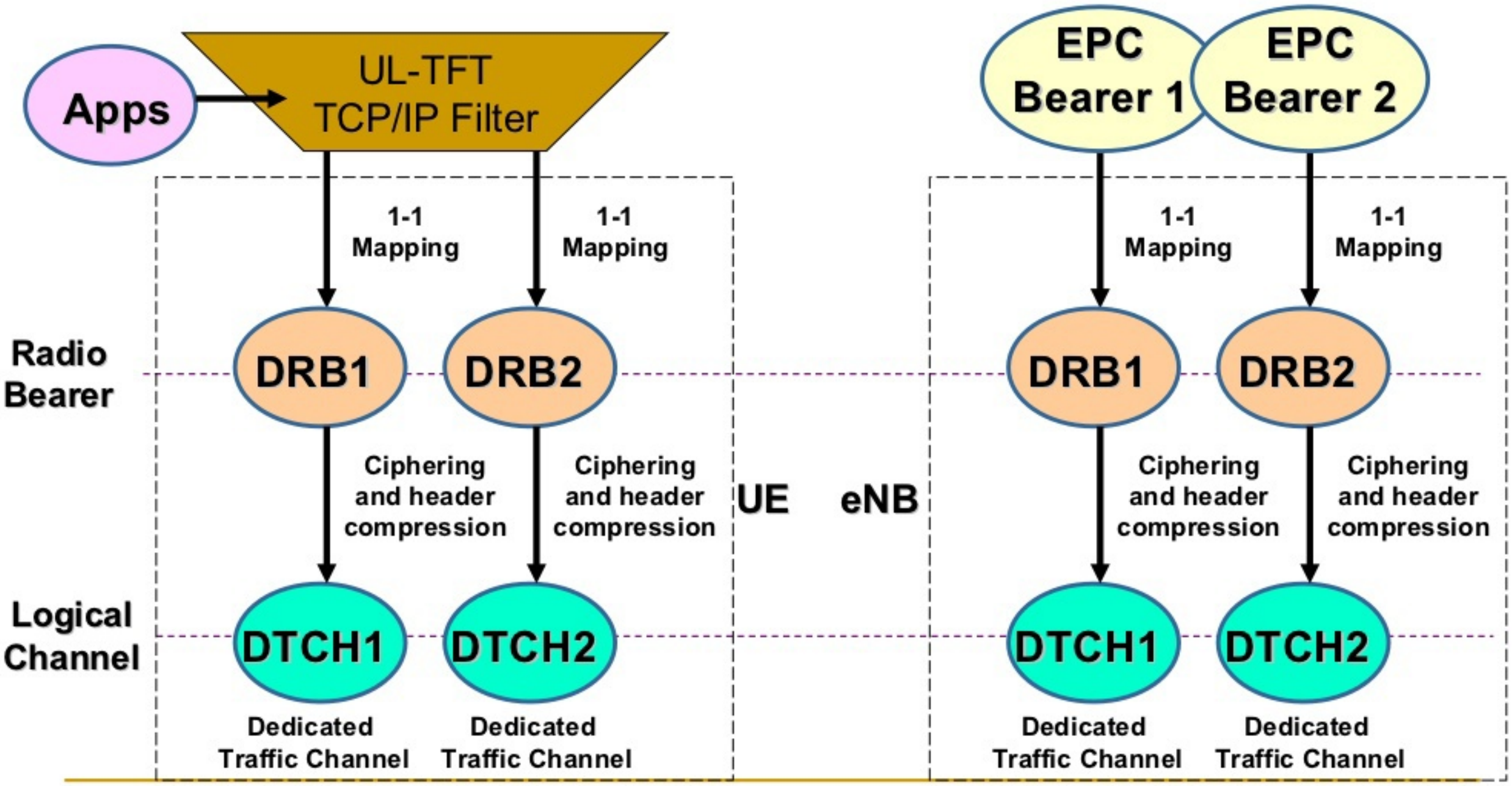
	1: Off	Attaching	2: Idle / Registered	Connecting To EPC	3: Active
EMM	Deregistered		Registered		
ECM	Idle				Connected
RRC	Idle	Connected	Idle	Connected	

Connection Establishment and Release

- RRC connection establishment involves:
  - RRC connection establishment:
    - Establishment of SRB1.
    - Transfer of NAS messages.
  - RRC connection reconfiguration:
    - Establishment of S1 connection.
    - Access Startum (AS) security.
    - Establishment of SRB2.
    - Establishment of one or more DRBs.

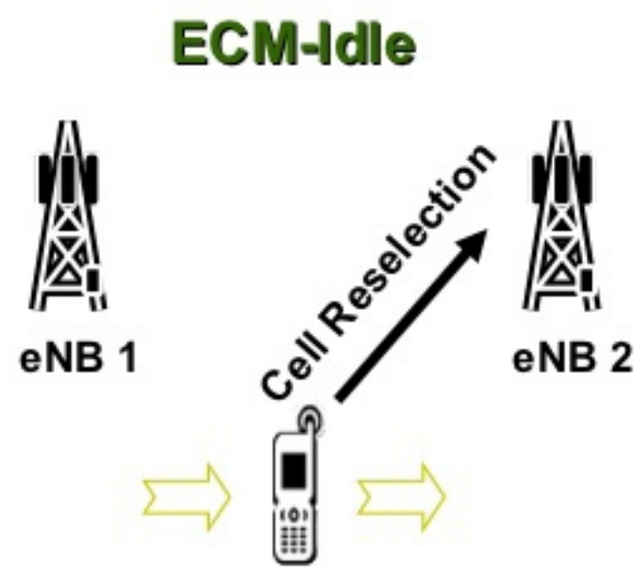


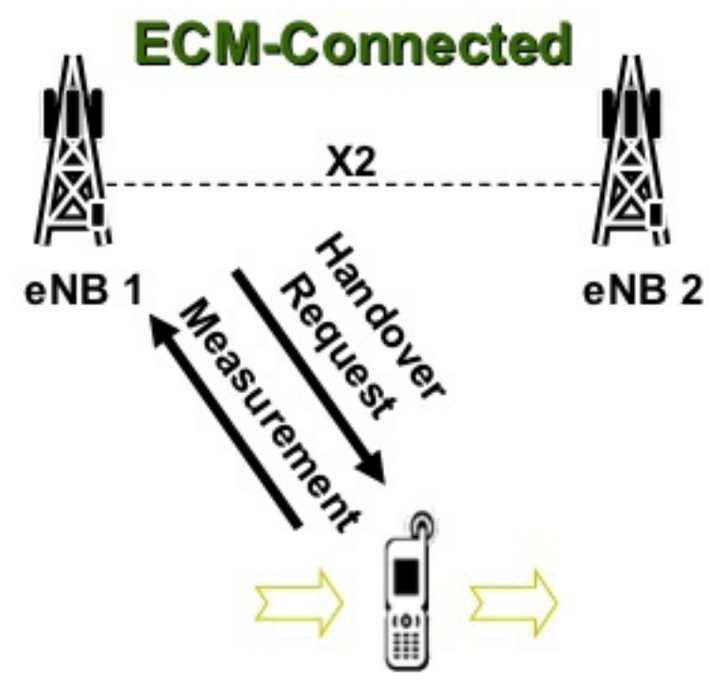
Radio Bearers Mapping



Mobility Control in RRC

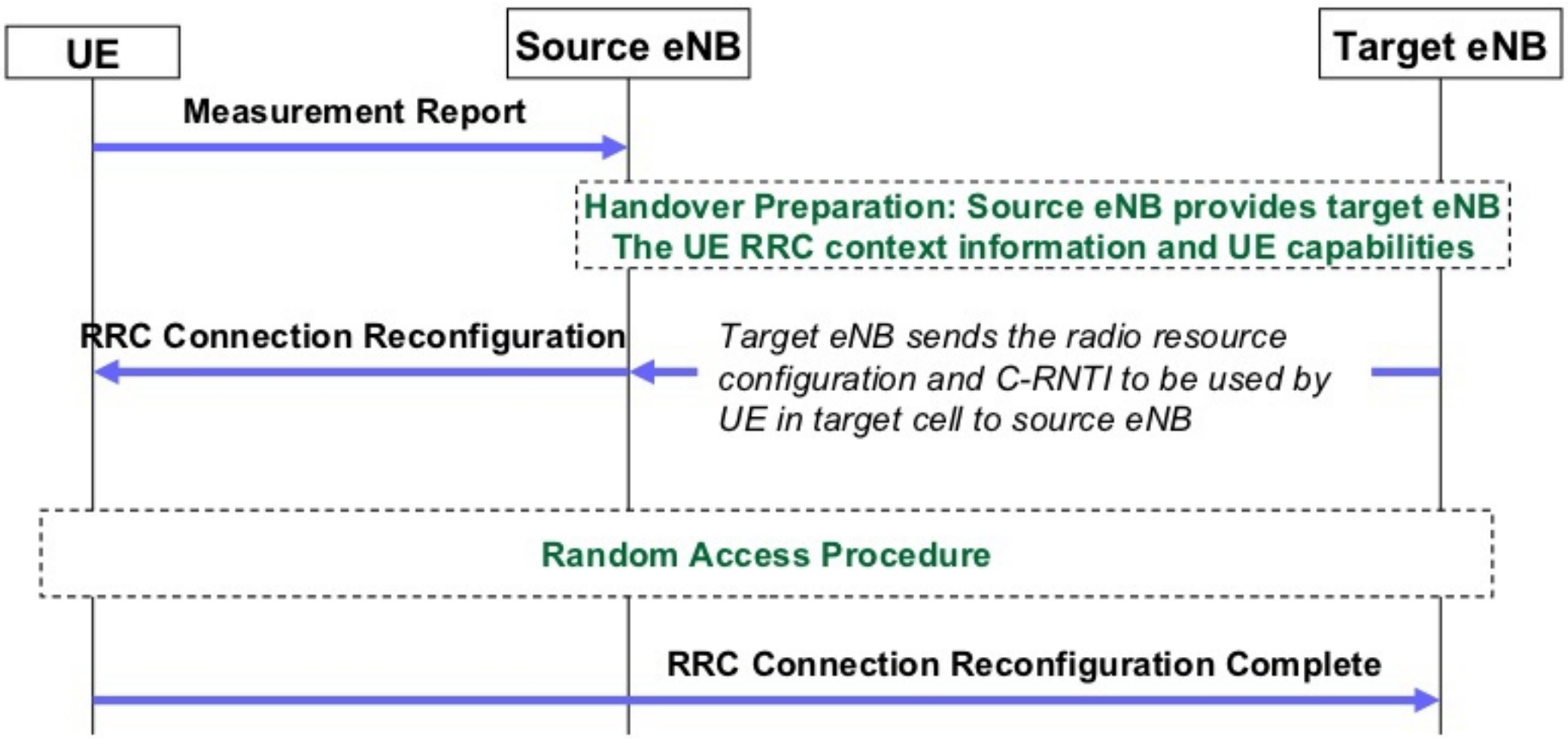
- Mobility Control depends on UE state:
  - UE in RRC-Idle: Mobility is UE-controlled (*cell-reselection*).
  - UE in RRC-Connected: Mobility is E-UTRAN controlled (*handover*).





Mobility in Connected Mode

- In LTE, UE always connects to a single cell only, in other words, *hard handover*.

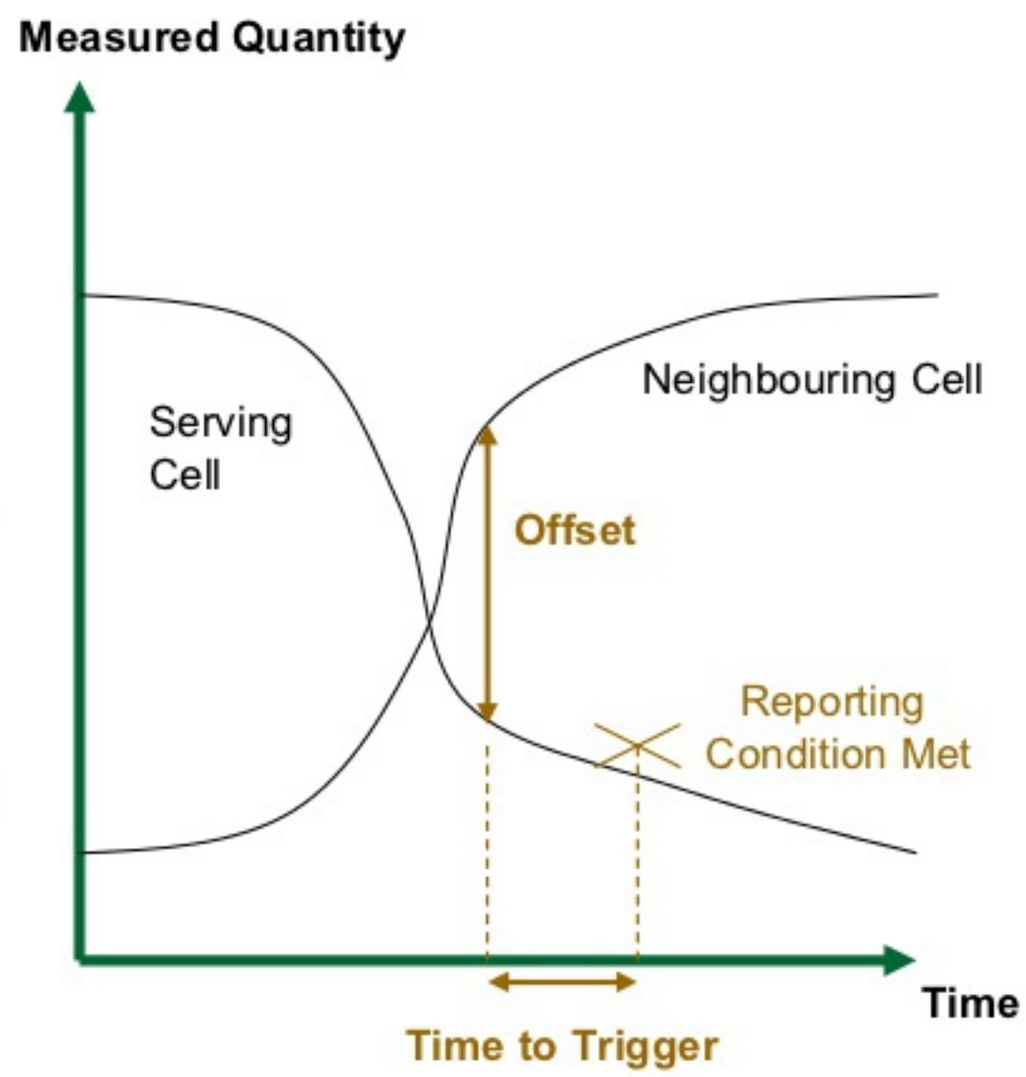


Measurements

- Measurement Objects:
  - Defines on what the UE performs the measurement, such as carrier frequency or cell ids.
- Measurement Reports:
  - Periodic or even-triggered measurement reports, as well as details of what UE is expected to report (RSRP or CQI).
  - Contains measurements for serving cells, listed cells, and detected cells on a listed frequency.

Measurements

- Measurements Events: (for event-triggered measurements)
  - Event A1: Serving cell becomes better than absolute threshold.
  - Event A2: Serving cell becomes worse than absolute threshold.
  - Event A3: Neighbour cell becomes better than an offset relative to serving cell.
  - Event A4: Neighbour cell becomes better than absolute threshold.



Cell Selection

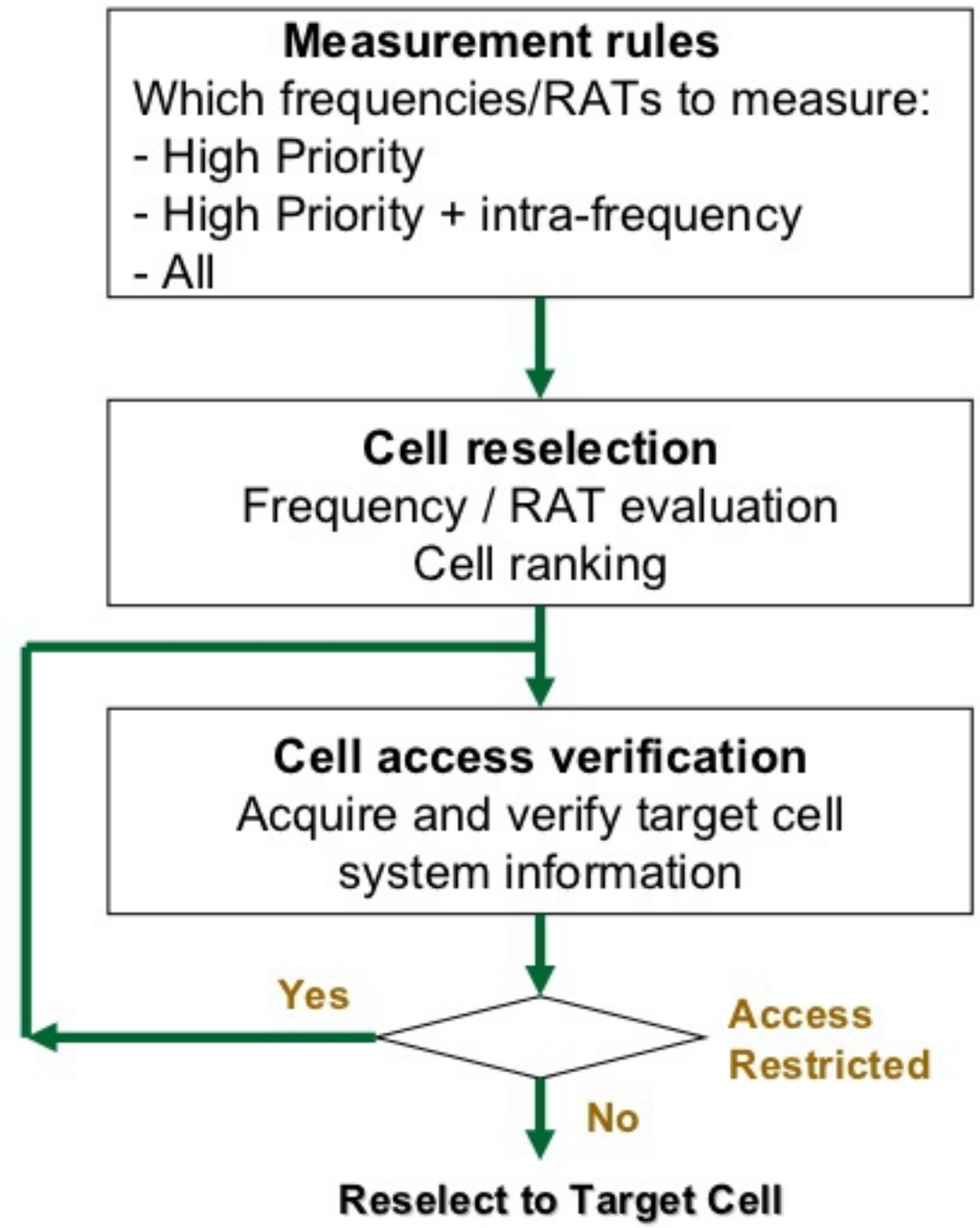
- Cell Selection consists of the UE searching for the strongest cell on all frequencies.
  - The main requirement for cell selection is that it should not take too long.
  - The cell selection criterion *S-criterion* is fulfilled when the cell-selection receive level $S_{rxlev} > 0$.

$$S_{rxlev} = Q_{rxlevmeas} - (Q_{rxlevmin} - Q_{rxlevminoffset})$$

$Q_{rxlevmeas}$: Measured cell receive level, aka RSRP.
$Q_{rxlevmin}$: Minimum required receive level.
$Q_{rxlevminoffset}$: An offset configured to favor H-PLMN and prevent ping-pong between PLMNs.

Cell Reselection

- Once UE camps on a suitable cell, it starts cell reselection. This process aims to move the UE to the best cell of the selected PLMN.
- UE first evaluates frequencies of all RATs based of their priorities, then UE compares cells based on radio quality *R-criterion*



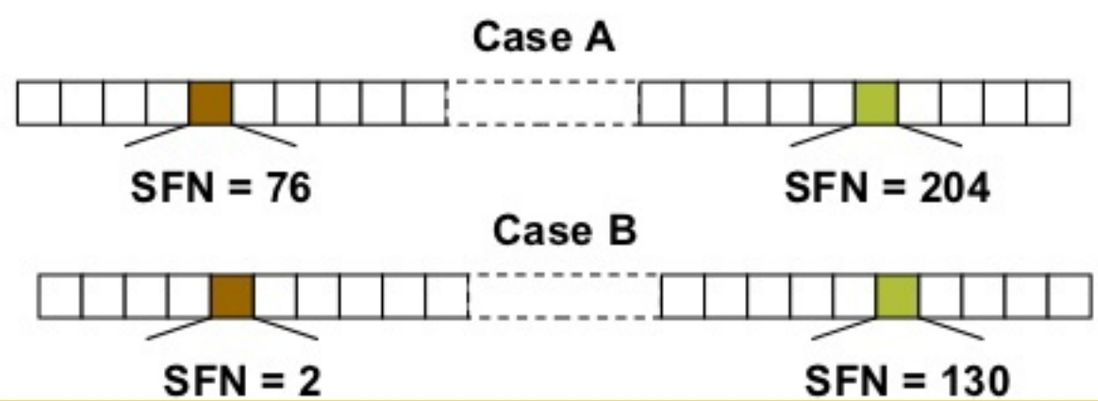
Paging

- To receive paging messages from E-UTRAN, UEs in idle mode monitor the PDCCH channel for Paging RNTI (P-RNTI).
- The UE only needs to monitor the PDCCH channel at certain UE-specific occasions.

$$SFN \bmod T = (T/N) \times (UE_ID \bmod N)$$

T : Minimum of cell-specific paging cycle and UE-specific paging cycle
N : Number of paging frames with the paging cycle of the UE.
UE_ID : IMSI mod 4096

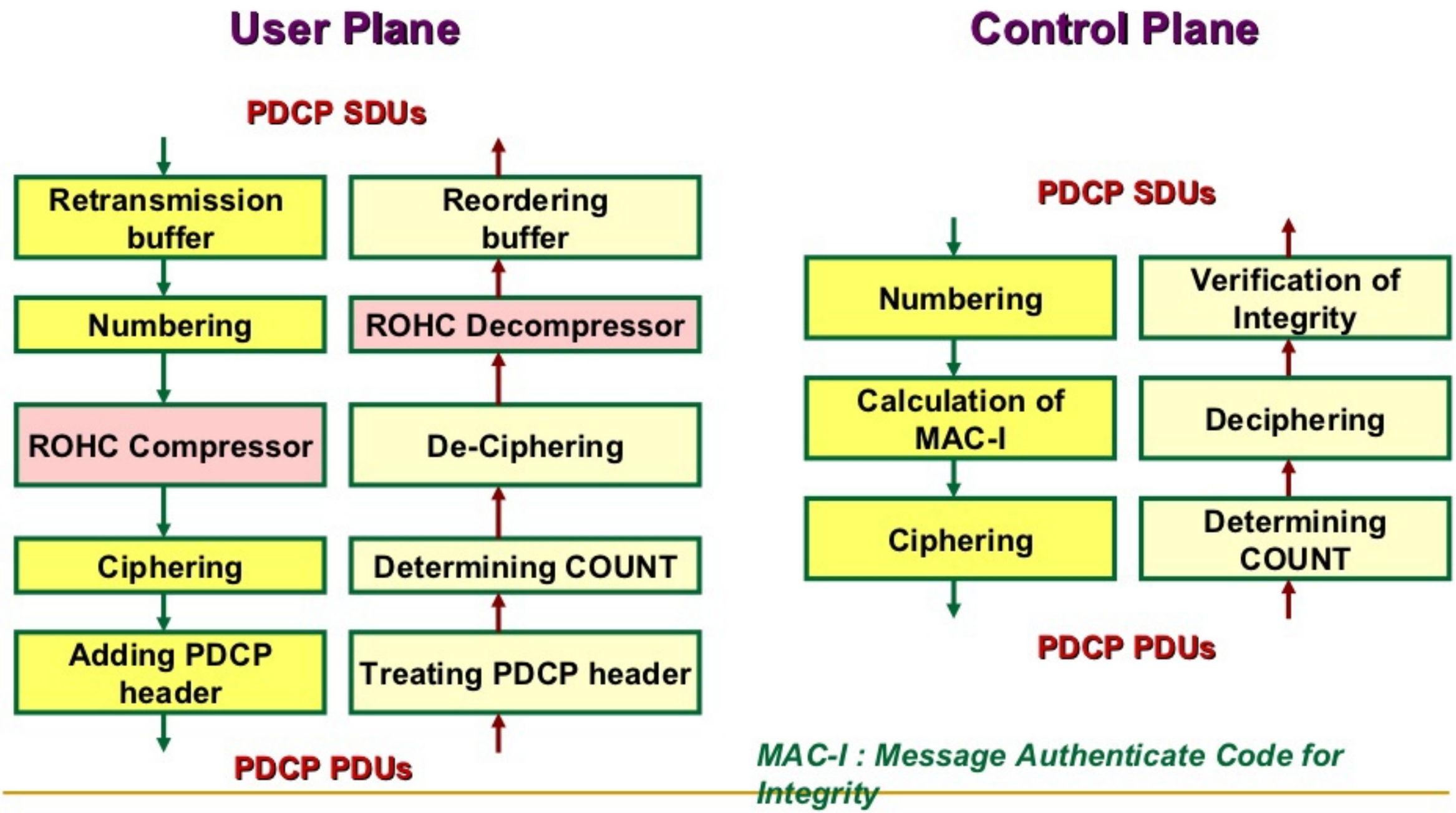
Case	T	N	UE_ID
A	128	32	147
B	128	128	147



User Plane Protocols

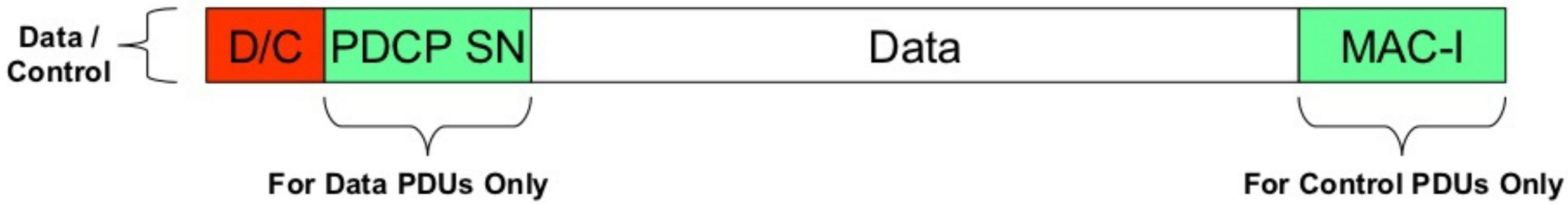
- LTE user-plane protocol stack is composed of three sub layers:
  - The Packet Data Convergence Protocol (PDCP):
    - Header Compression, security (integrity protection and ciphering), and support of reordering and retransmission during handover, there is one PDCP entity per radio bearer.
  - The Radio Link Control (RLC):
    - Segmentation and assembly of upper layer packets. Retransmission and reordering of packets using HARQ. One RLC entity per radio bearer.
  - The Medium Access Control (MAC):
    - Multiplexing of data from different radio bearers. One MAC entity per UE.

PDCP Layer

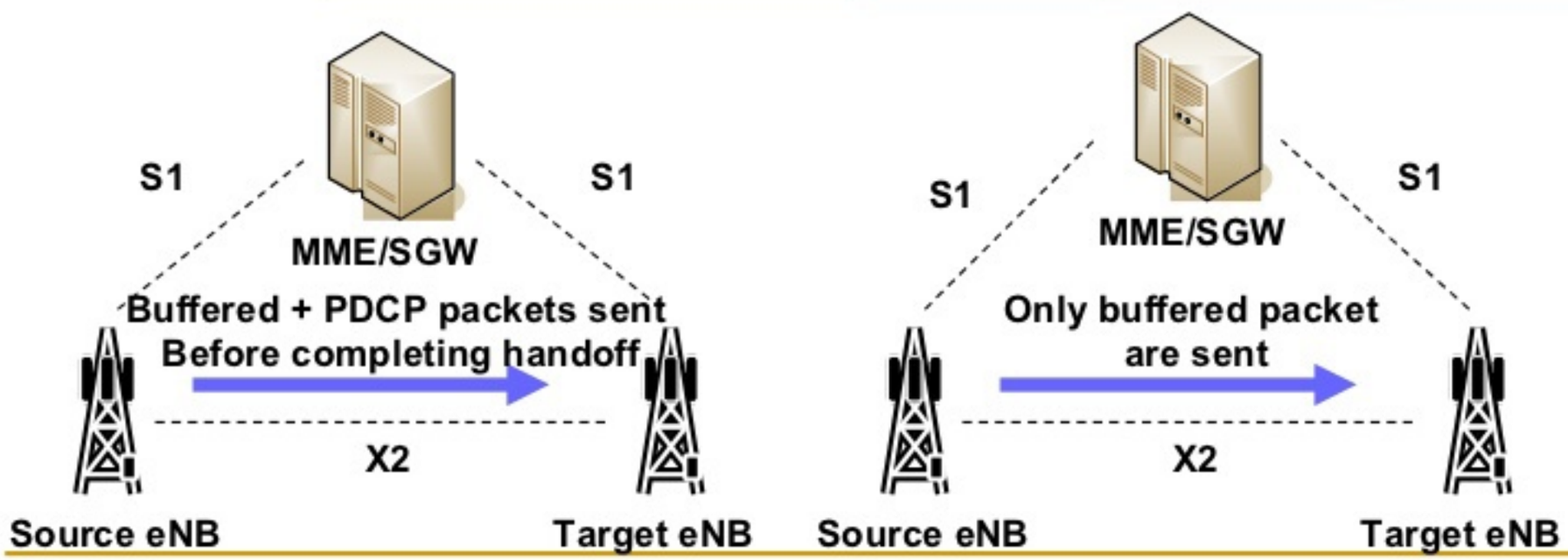


MAC-I : Message Authenticate Code for Integrity

PDCP PDU Format



PDU Type	D/C Field	SN Length	MAC-I	RLC Modes
User Plane Long SN	Present	12 bits	Absent	AM / UM
User Plane Short SN	Present	7 bits	Absent	UM
Control Plane	Absent	5 bits	32 bits	AM / UM

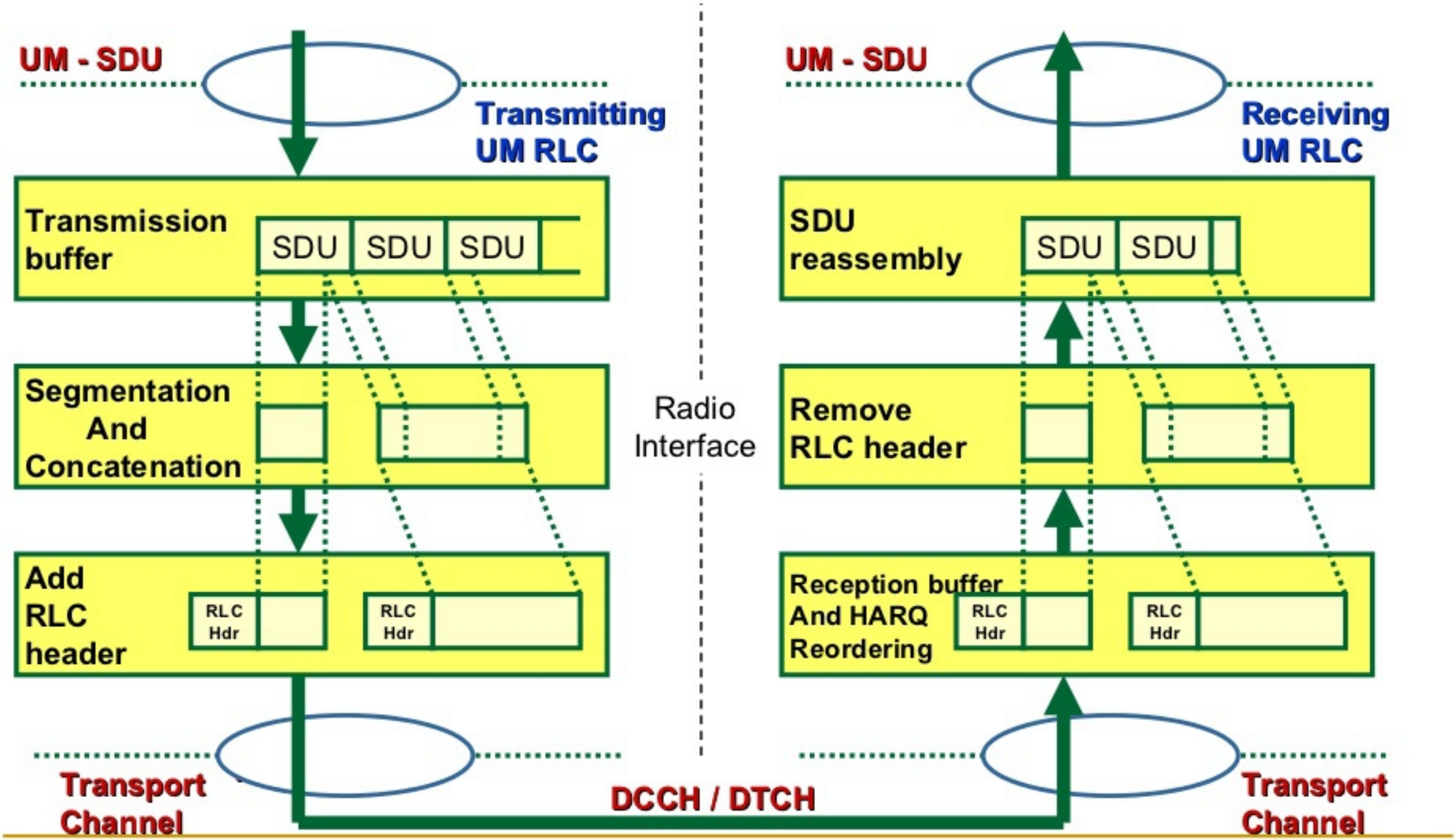


PDCP in Handover

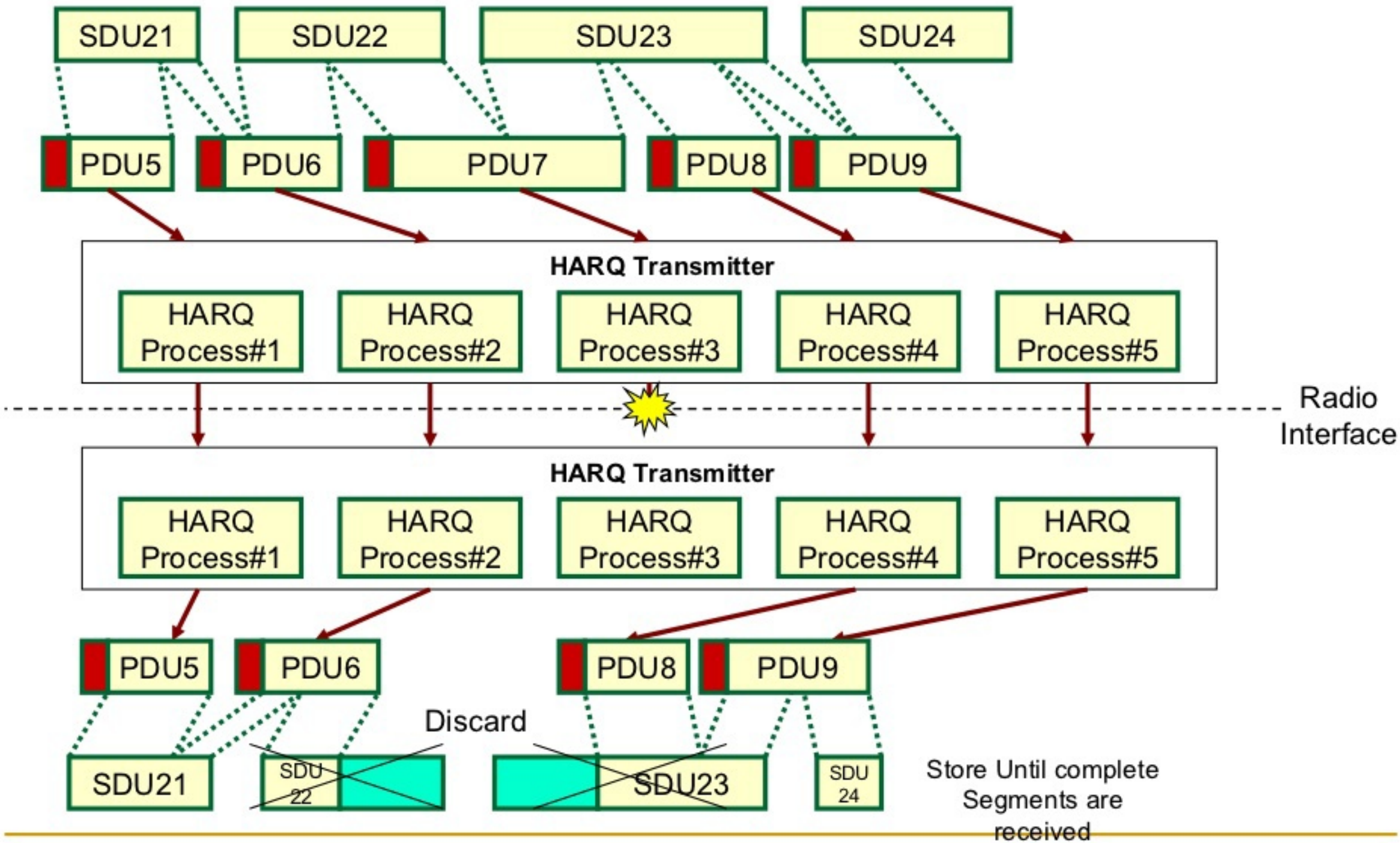
RLC Layer

- RLC transmission modes:
  - Transparent Mode (TM):
    - RLC is transparent to TM PDUs; no RLC header is added. Used for Broadcast SI messages, paging , and SIB0 messages.
  - Unacknowledged Mode (UM):
    - Used for delay-sensitive real-time applications such as VOIP and MBMS. Packets are reordered and reassembled.
  - Acknowledged Mode (AM):
    - Used for error-sensitive and delay-tolerant applications. Retransmission of packets using HARQ.

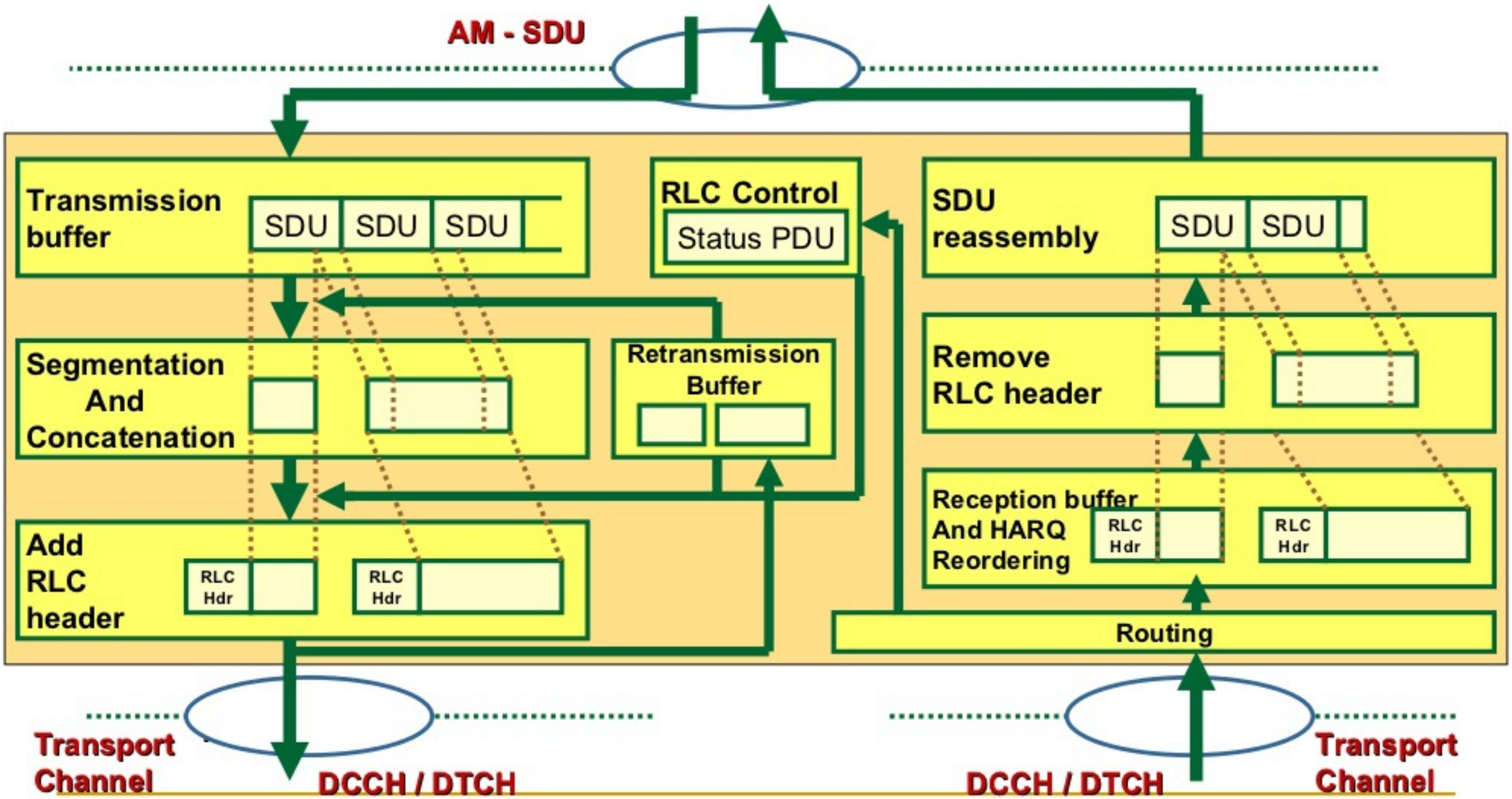
Unacknowledged Mode



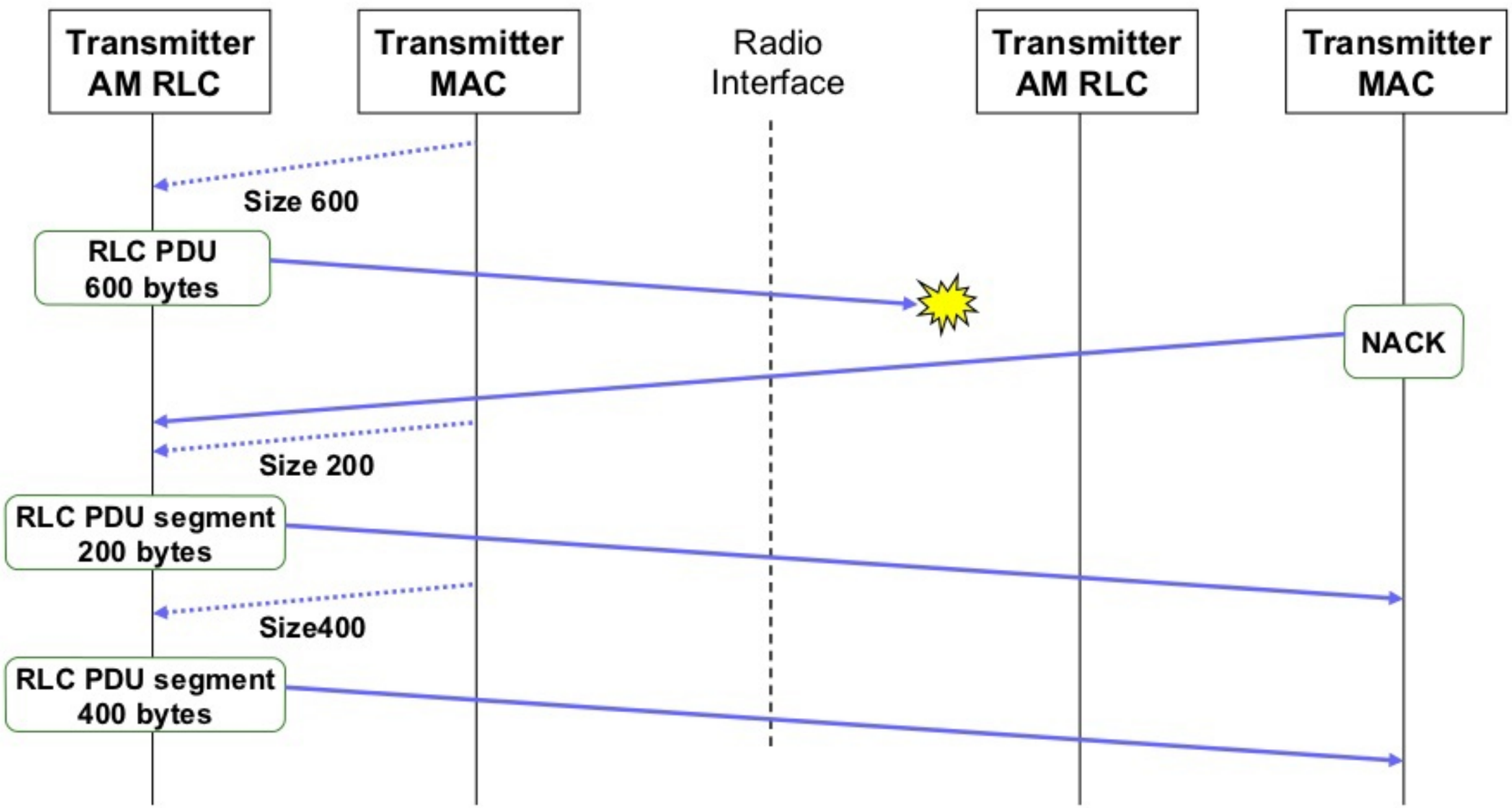
UM HARQ Loss Detection & Reordering



Acknowledged Mode

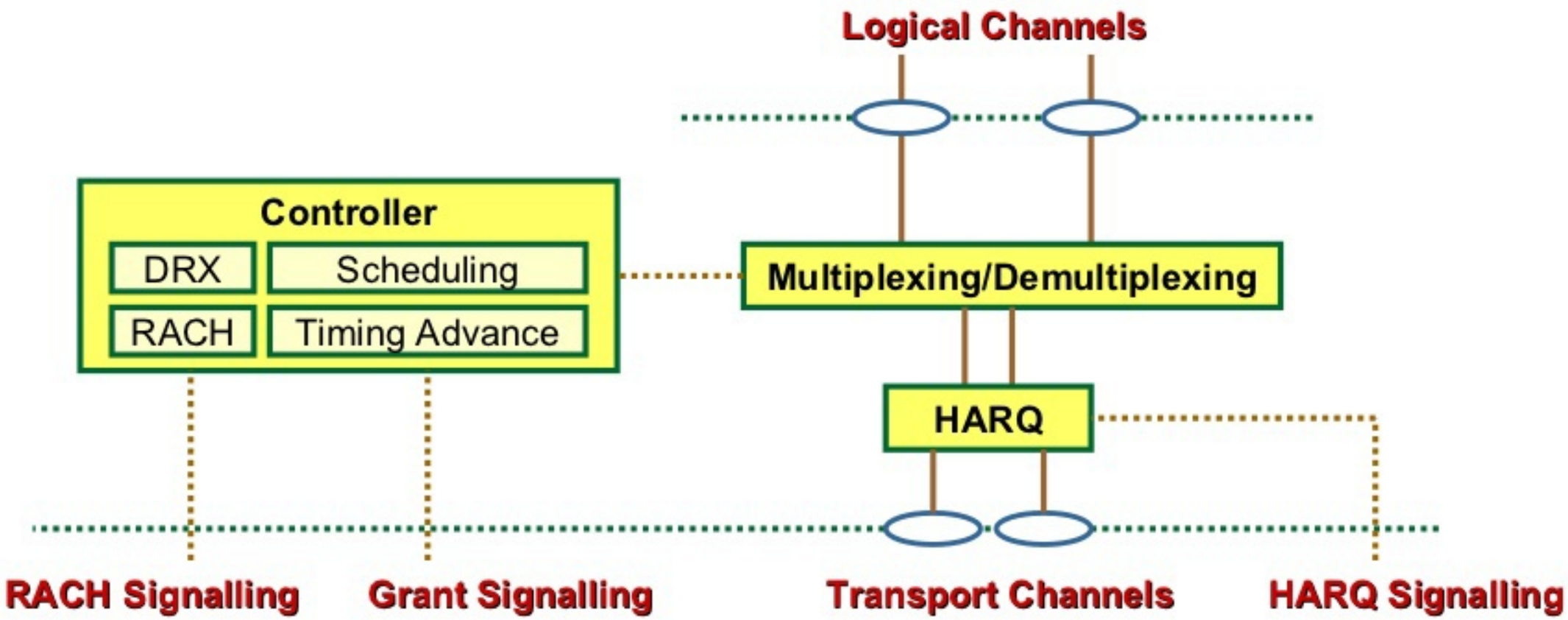


Acknowledged Mode Retransmission



Media Access Control (MAC) Layer

- Performs multiplexing and demultiplexing between logical channels and transport channels.



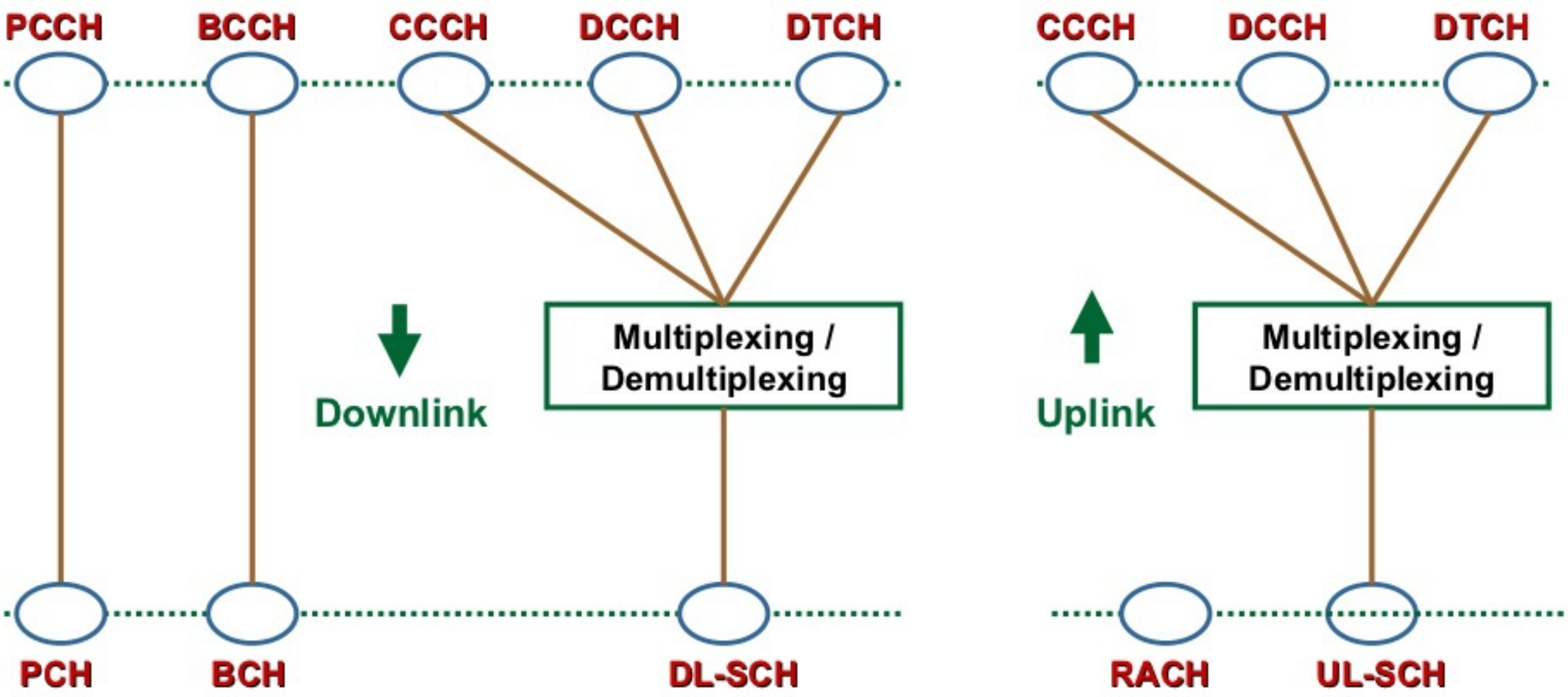
Logical Channels

- Broadcast Control Channel (BCCH):
  - DL-Ch to broadcast system information. TM RLC mode.
- Paging Control Channel (PCCH):
  - DL-Ch to notify UEs of incoming call.
- Common Control Channel (CCCH):
  - UL/DL-Ch to deliver control information when UE has no association with eNodeB. TM RLC mode.
- Dedicated Control Channel (DCCH):
  - UL/DL-Ch to deliver control information when UE has RRC connection with eNodeB. AM RLC mode.
- Dedicated Traffic Channel (DTCH):
  - UL/DL-Ch to transmit dedicated user data. UM or AM RLC mode.

Transport Channels

- Downlink Transport Channels:
  - Broadcast Channel (BCH).
  - Downlink Shared Channel (DL-SCH).
  - Paging Channel (PCH).
  - Multicast Channel (MCH).
- Uplink Transport Channels:
  - Uplink Shared Channel (UL-SCH).
  - Random Access Channel (RACH).

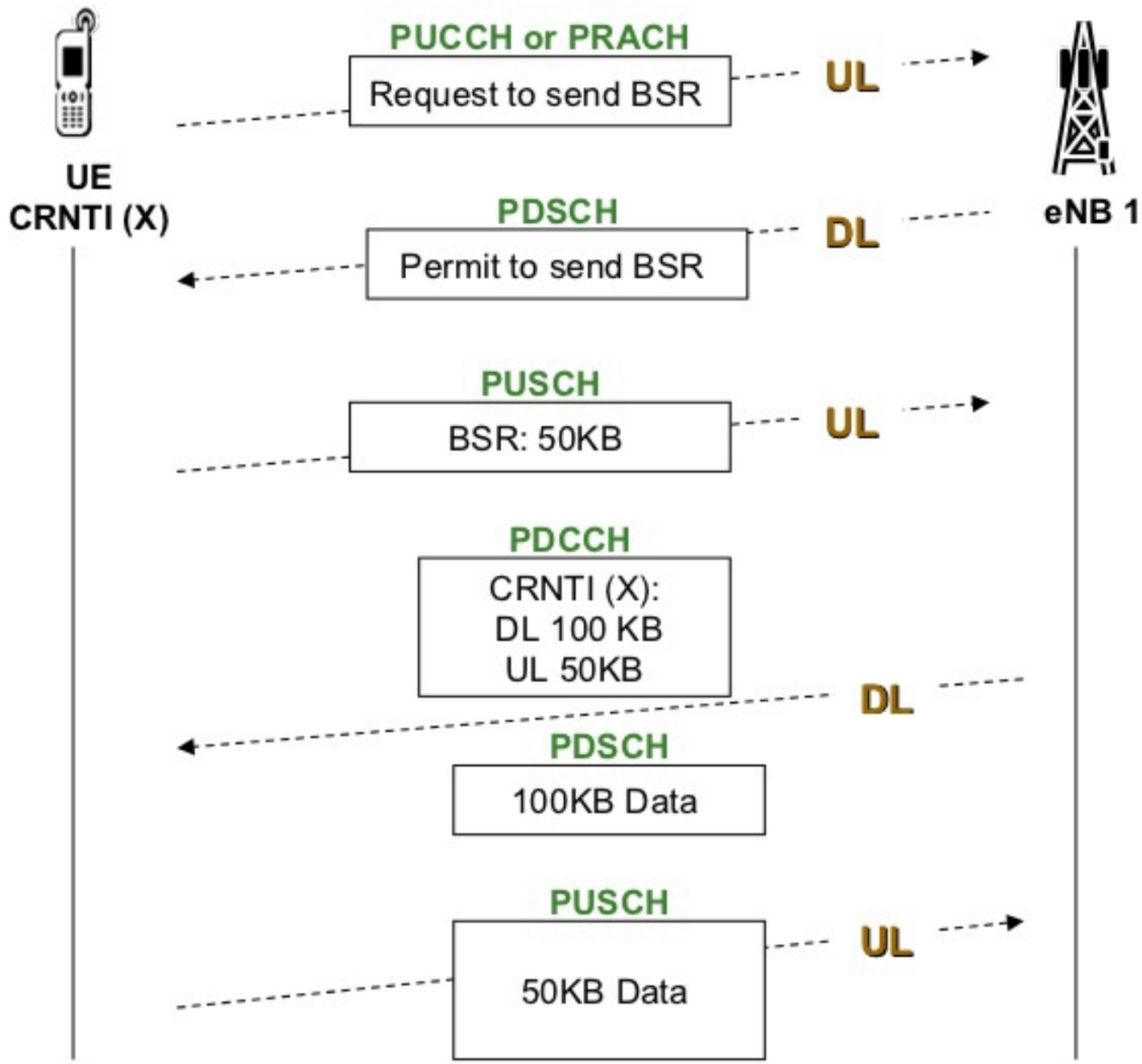
Multiplexing Between Logical Channels and Transport Channels



MAC Functions

- Scheduling:
  - Distributes available radio resources among UEs.
  - Resources allocation is based on Buffer Status Reports (BSRs) received from UEs.
  - Dynamic Scheduling:
  - DL assignment messages for downlink allocation and UL grant messages for uplink allocation, both transmitted over the Physical Downlink Control Channel (PDCCH) using a Cell Radio Network Temporary Id (C-RNTI).

MAC Resources Scheduling



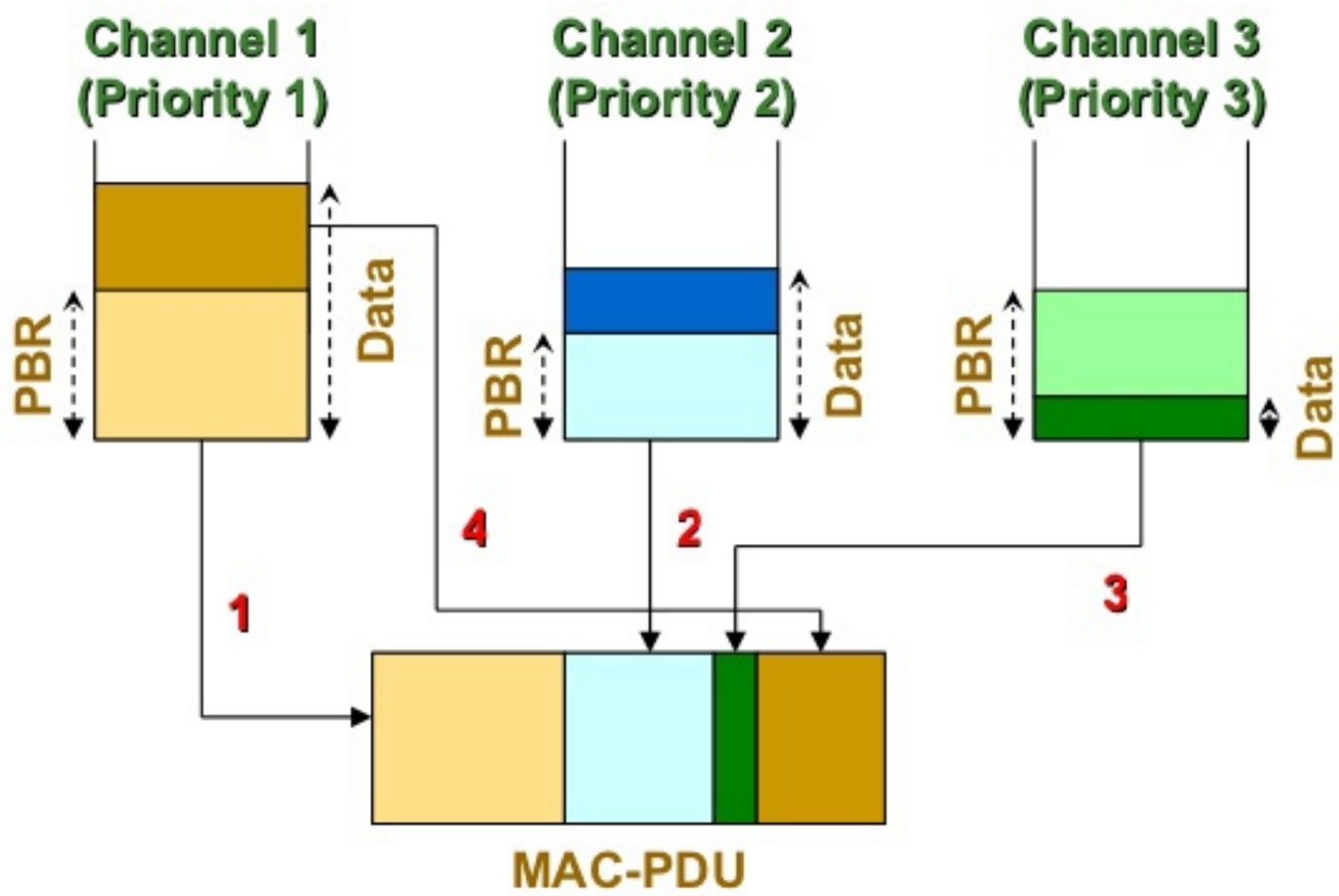
UL: 50KB
DL: 100KB

MAC Functions

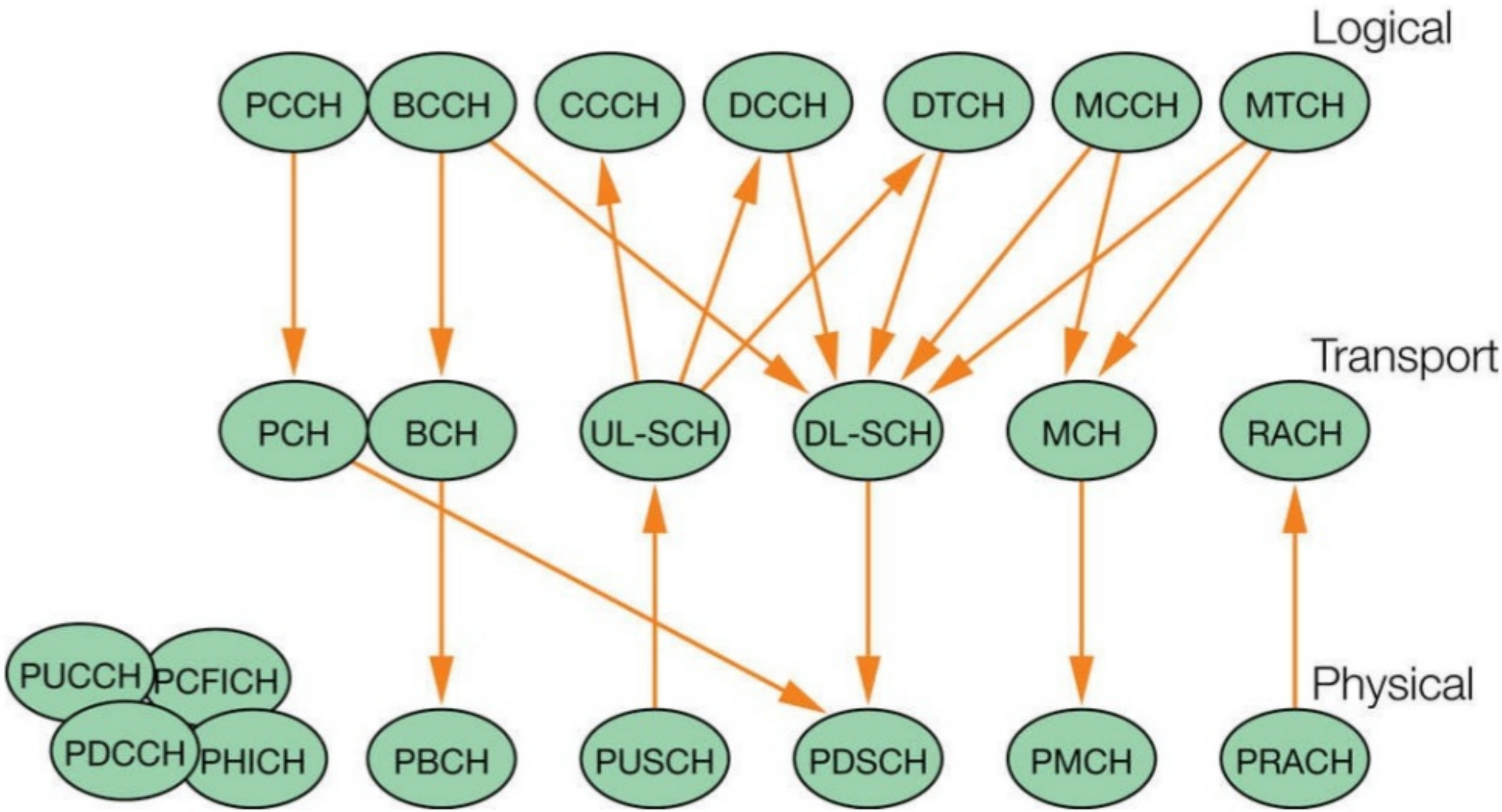
- Random Access Procedure:
  - Used when UE is not allocated with uplink radio resources but has something to transmit.
  - Used for UE initial network attach, UE moving out of RRC_Idle, UE has UL data to send, and when uplink synchronization is lost.
- Uplink Timing Alignment:
  - Used to ensure UE's uplink transmission arrive at eNodeB without overlapping with other UE's transmission.

MAC Multiplexing and Prioritization

- Prioritized Bit Rate (PBR): Data rate provided to one logical channel before allocating any resource to a lower-priority channel.



MAC Physical Channels



Further Readings

- 3GPP Technical Specification 36.323, “Packet Data Convergence Protocol (PDCP) Specification (Release 8)”, www.3gpp.org.
- 3GPP Technical Specification 36.322, “Radio Link Control (RLC) Protocol Specification (Release 8)”, www.3gpp.org.
- 3GPP Technical Specification 36.321, “Medium Access Control (MAC) Protocol Specification (Release 8)”, www.3gpp.org.

LTE

3GPP Standard Perspective
Chapter 4 – Air Interface

Muhannad Aulama

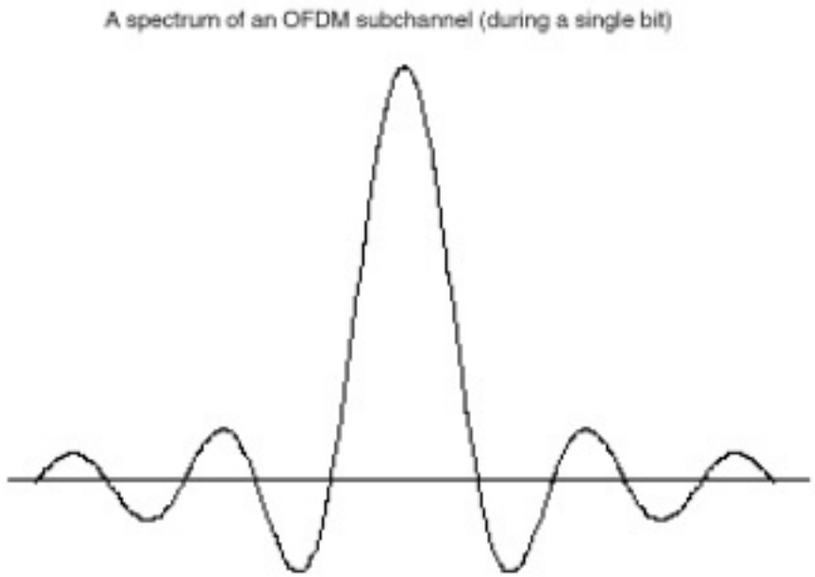
Contents of Chapter 4

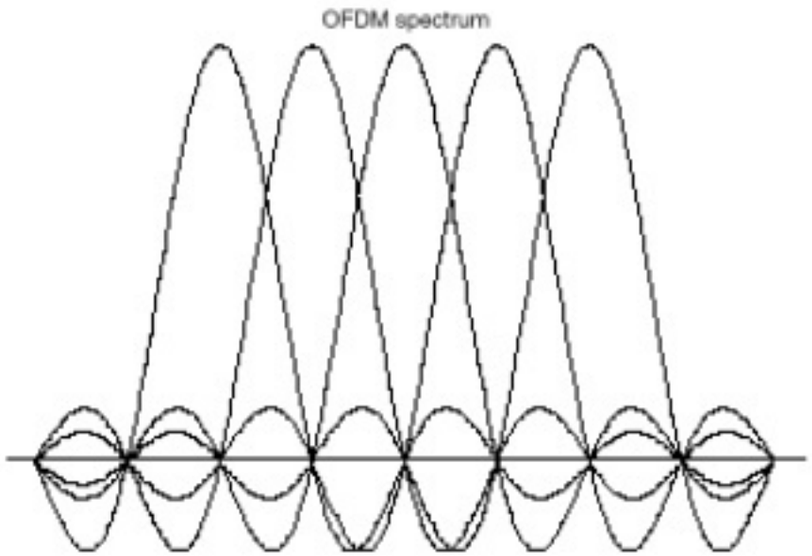
- Introduction.
- OFDMA.
- Inter-symbol Interference.
- Disadvantages of OFDMA .
- Channel Bandwidth.
- FDD Radio Frame.
- TDD Radio Frame.
- Resource Block.
- Synchronization and Cell Search.
- Reference Signals and Channel Estimation.
- Downlink Physical Channels Mapping.
- Constellations of Modulation Schemes.
- Layer 1 Downlink Physical Control Channels.
- Channel Coding and Link Adaptation.
- Channel Quality Indicator Mapping.
- LTE Measurements.
- Uplink Physical Channel Mapping.
- Layer 1 Uplink Physical Control Channels.
- Random Access Procedure.
- Multiple Antenna Techniques.
- Advantages of Multiple Antennas.
- SU-MIMO vs MU-MIMO.
- Beamforming Schemes.
- LTE Transmission Modes.
- Further Readings.

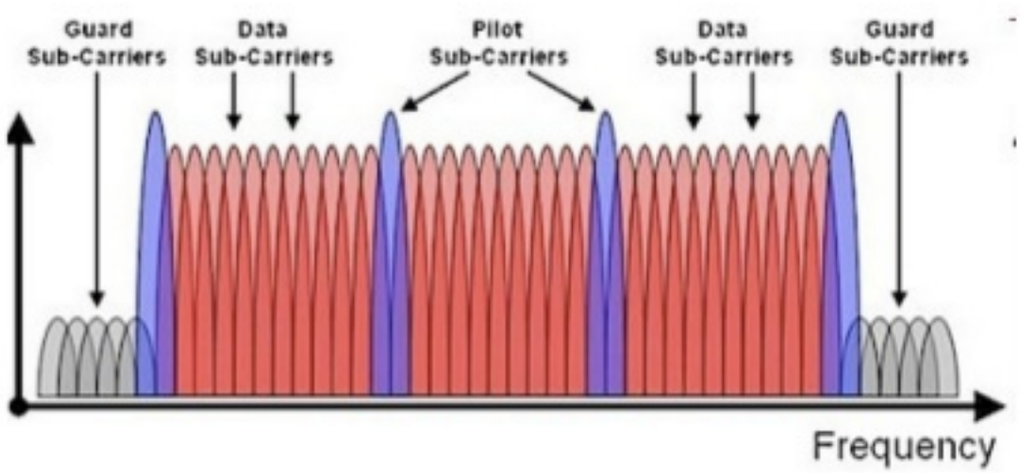
Introduction

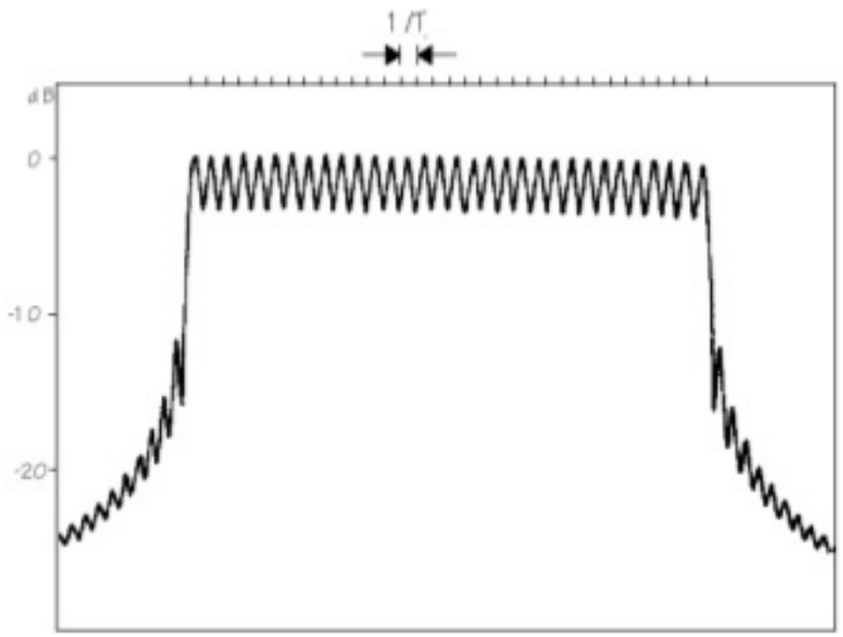
- LTE is using OFDMA (Orthogonal Frequency Division Multiple Access) as the modulation and multiple-access technique for mobile wireless communication over the air in the downlink direction.
- OFDMA divides the frequency wideband channel into overlapping but orthogonal narrowband sub-channels, avoiding the need to separate the carriers by guard-bands making OFDMA highly spectrum efficient.
- The spacing between sub-channels in OFDMA is such they can be perfectly separated at the receiver.

OFDMA


A spectrum of an OFDM subchannel (during a single bit)


OFDM spectrum

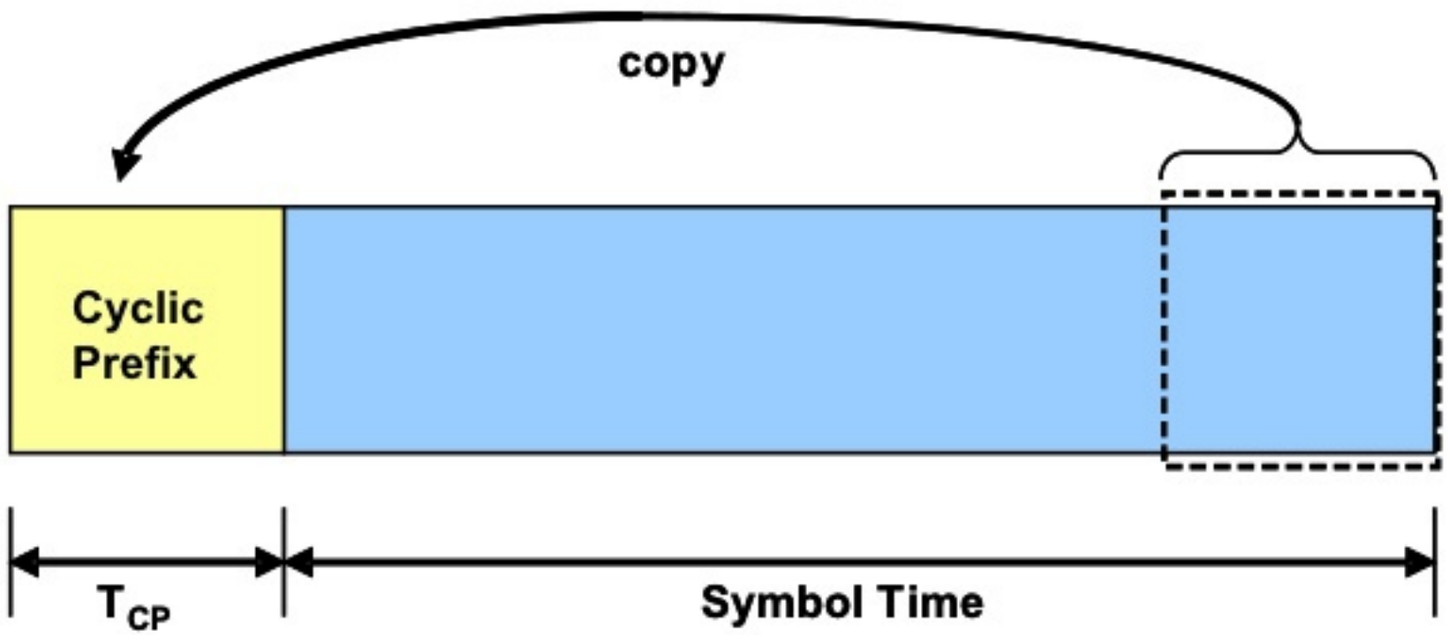

Guard
Sub-Carriers
Data
Sub-Carriers
Pilot
Sub-Carriers
Data
Sub-Carriers
Guard
Sub-Carriers
Frequency


1 /T
dB
0
-10
-20

Inter-symbol Interference

- High-rate data streams faces a problem in having symbol period Ts much smaller than channel delay spread Td resulting in Inter-symbol Interference (ISI).
- In OFDM, the high-rate data stream is first serial-to-parallel converted for modulation into M parallel sub-carriers, increasing symbol duration on each sub-carrier significantly longer than channel delay spread.
- Due to multi-path propagation, a guard period is added at the beginning of each OFDM symbol. The guard period is obtained by adding a Cyclic Prefix (CP) at the beginning of the symbol.

Inter-symbol Interference

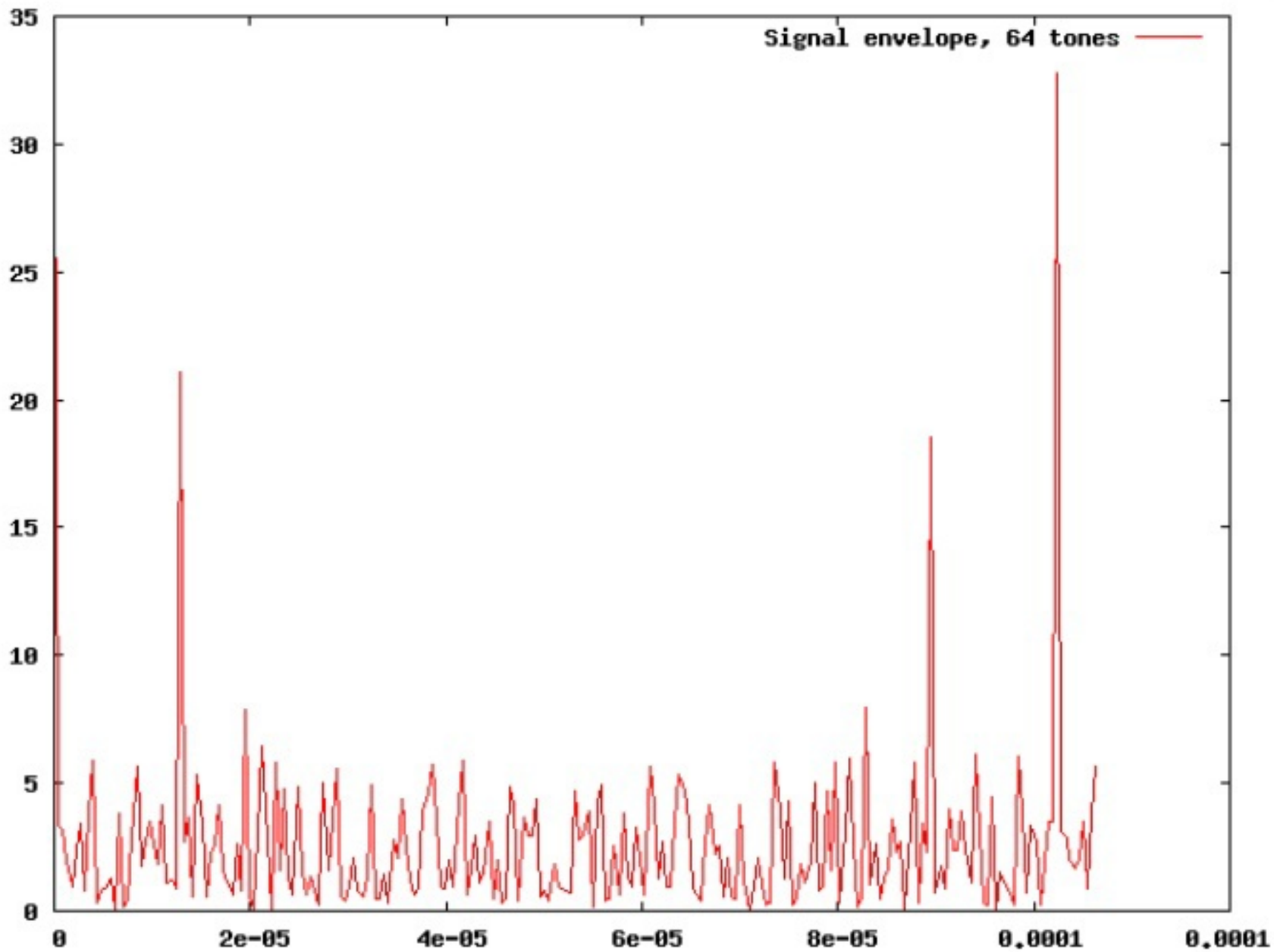


- LTE defined two cycle prefix sizes: normal and extended, 5 msec and 16.67 msec respectively.

Disadvantages of OFDMA

- The time-domain OFDM symbol can be approximated as a Gaussian waveform, therefore the amplitude variation of the OFDM modulated signal can be very high, which is called high Peak-to-Average Power Ratio (PAPR).
- However, Power Amplifiers (PA) of RF transmitters are linear only within a limited range. Thus OFDM signal is likely to suffer from non-linear distortion caused by clipping.
- SC-FDMA is used in uplink to avoid PARP in UEs.

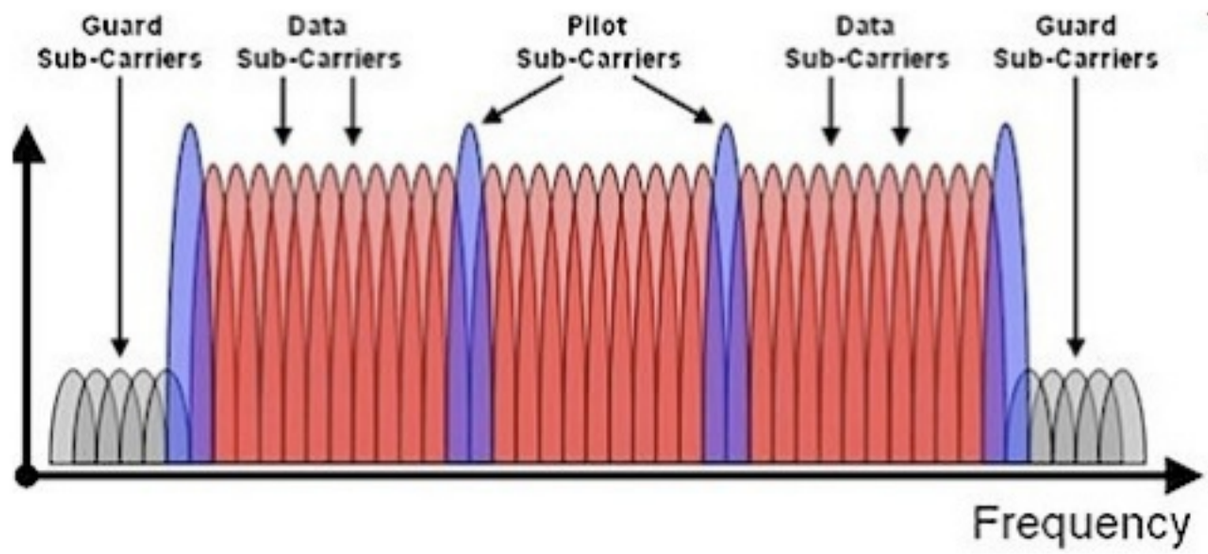
Disadvantages of OFDMA



Channel Bandwidth

- LTE is flexible to various channel bandwidths: 1.4MHz, 3MHz, 5MHz, 10MHz, 15MHz, and 20MH.
- All channel bandwidths have same 15KHz sub-carrier spacing, only FFT size is changed (number of sub-carriers).
- Sub-carriers types: DC sub-carrier, Guard sub-carrier, Data sub-carrier, and Reference sub-carrier.

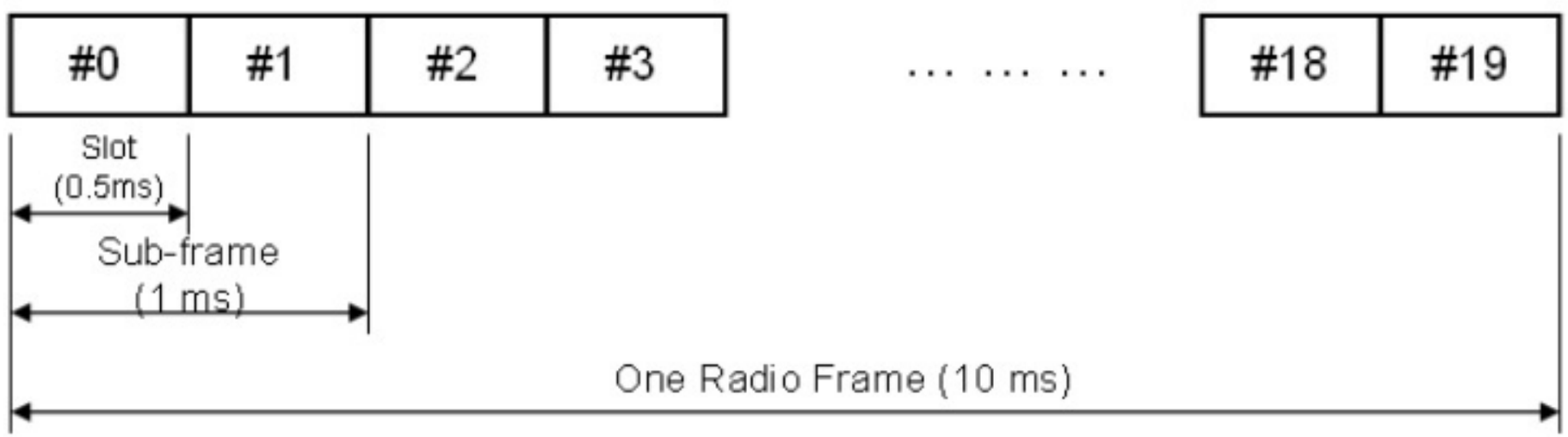
Channel Bandwidth



	Channel Bandwidth					
	1.4 MHz	**3 MHz**	**5 MHz**	**10 MHz**	**15 MHz**	**20 MHz**
Sampling Frequency (MHz)	1.92	3.84	7.68	15.36	23.04	30.72
Number of Subcarriers (FFT size)	128	256	512	1024	1536	2048
Subcarrier Spacing (kHz)	15 (7.5 used in MBMS-dedicated cell)					
Number of Occupied Subcarriers (data and reference, not DC or guard)	72	180	300	600	900	1200
Subframe Duration (ms)	1					
Number of Resource Blocks (per slot)	6	15	25	50	75	100
Number of OFDM symbols per subframe (Short/Long CP)	14/12					

FDD Radio Frame

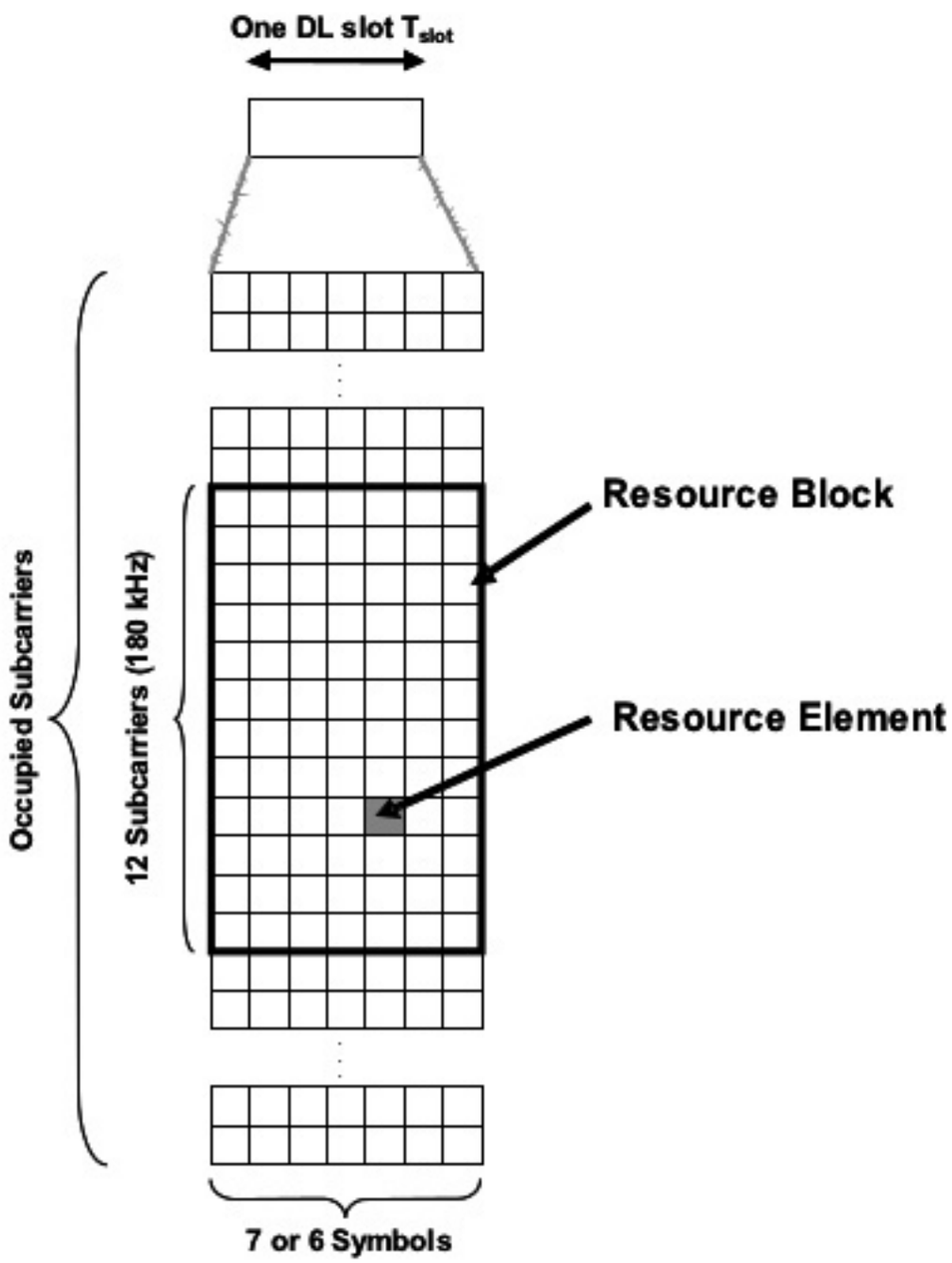
- LTE frame is 10 ms long, contains ten sub-frames 1 ms each. Each sub-frame contains two slots 0.5 ms each.

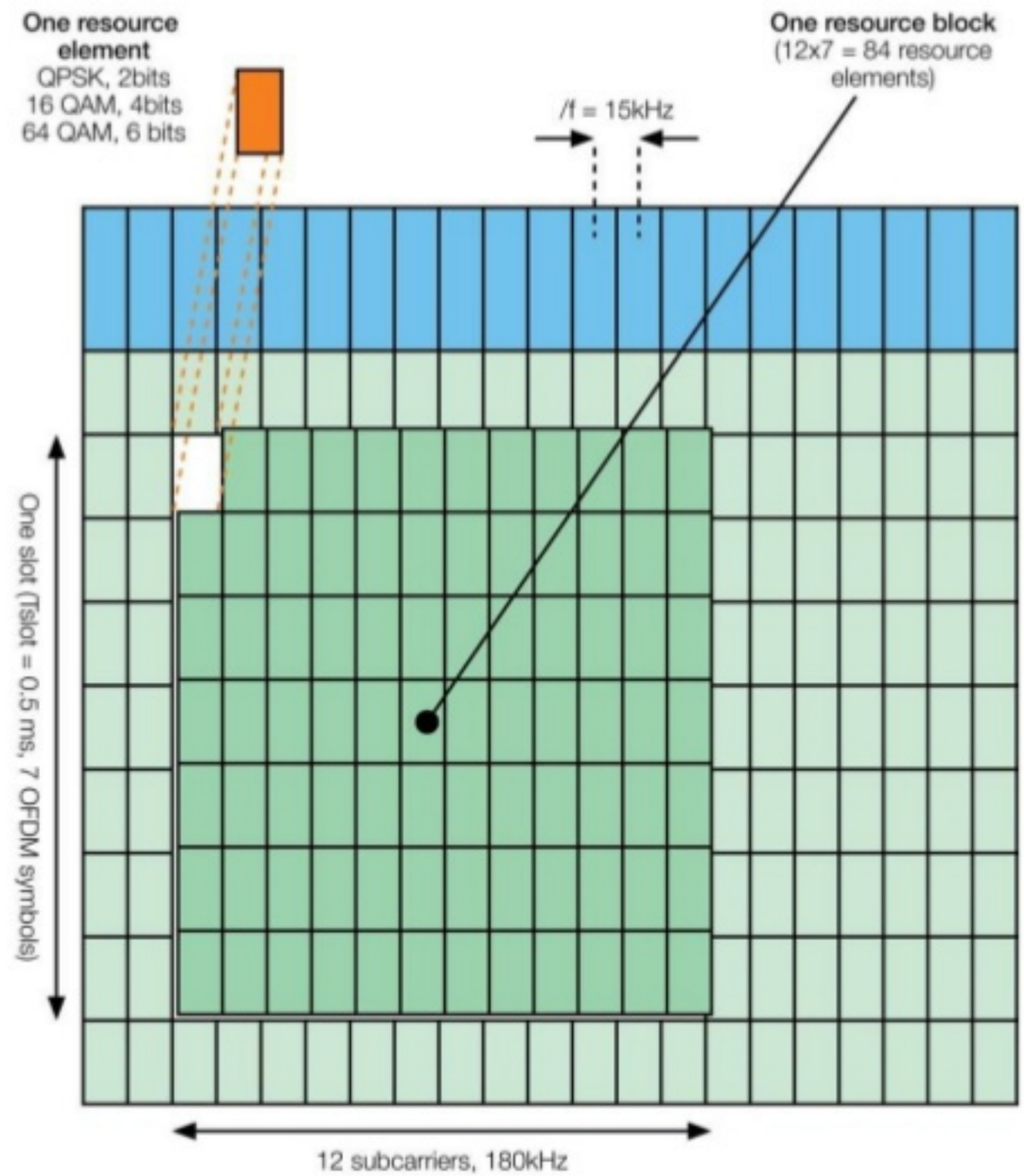


Resource Block

- The smallest unit of resource is the Resource Element (RE): 1 sub-carrier for a duration of 1 symbol.
- The unit of 12 sub-carriers for a duration of one slot (7 symbols) is Resource Block (RB).
- For 5MHz channel BW, number of resource blocks per slot is 25 (300 sub-carrier/12).

Resource Block

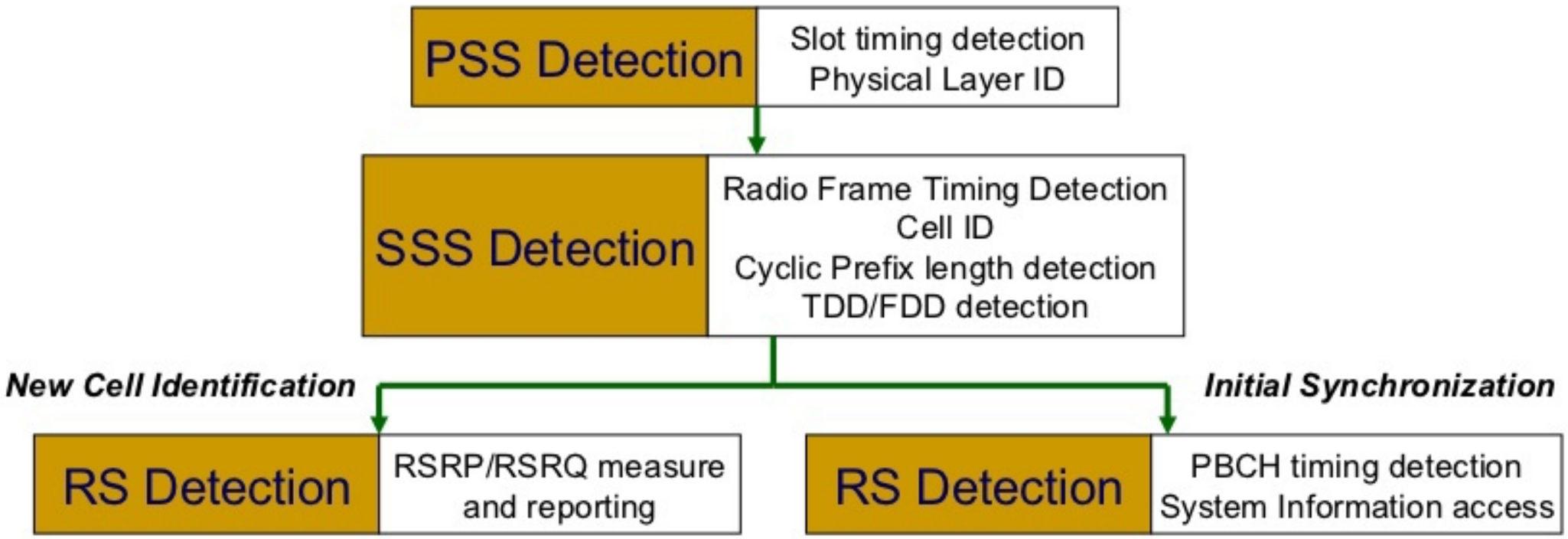


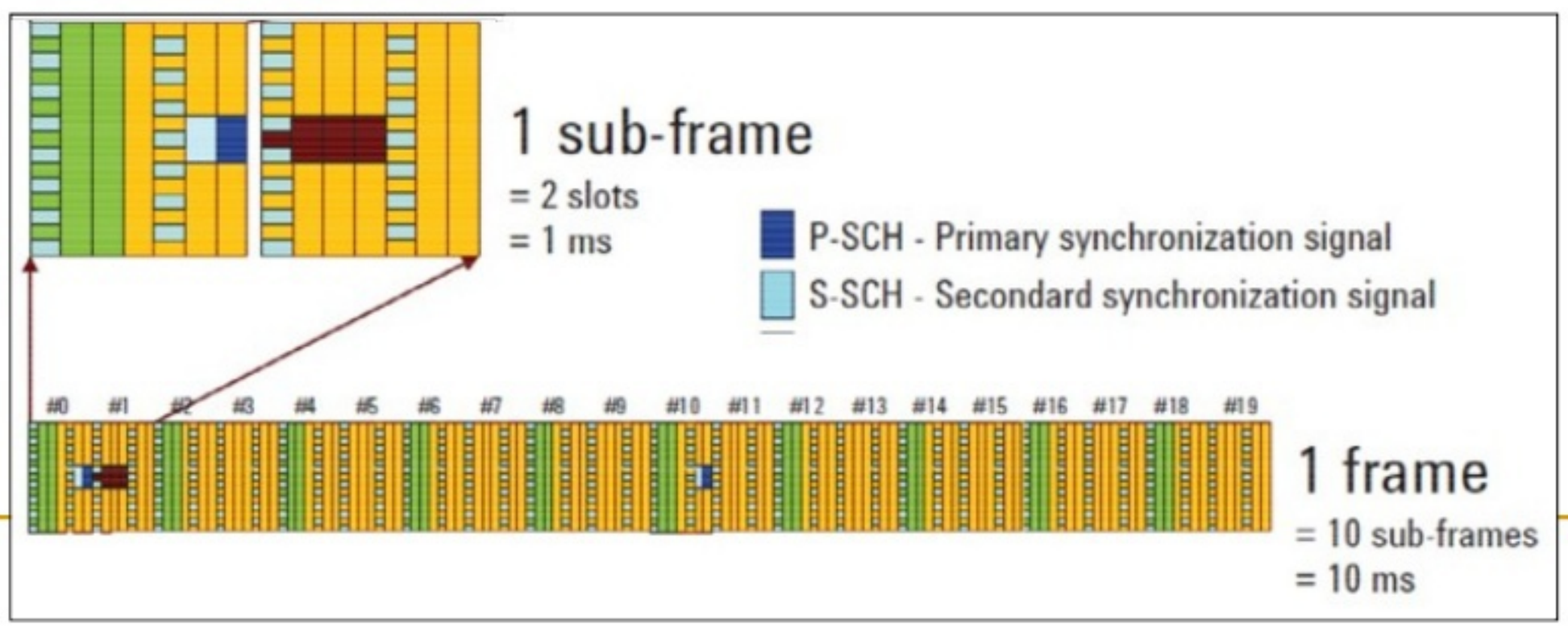


Synchronization and Cell Search

- Two relevant cell search procedures in LTE:
  - Initial synchronization: when UE is switched on or when it has lost the connection to the serving cell.
  - New cell identification: when UE is already connected to LTE cell and is in the process of detecting a new neighbour cell. The UE reports to the serving cell measurements related to the new cell.
- The synchronization process makes use of two specially designed physical signals: Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS).
- The detection of PSS and SSS provides UE with time and frequency sync, cyclic prefix length, and FDD/TDD frame type.

Synchronization and Cell Search



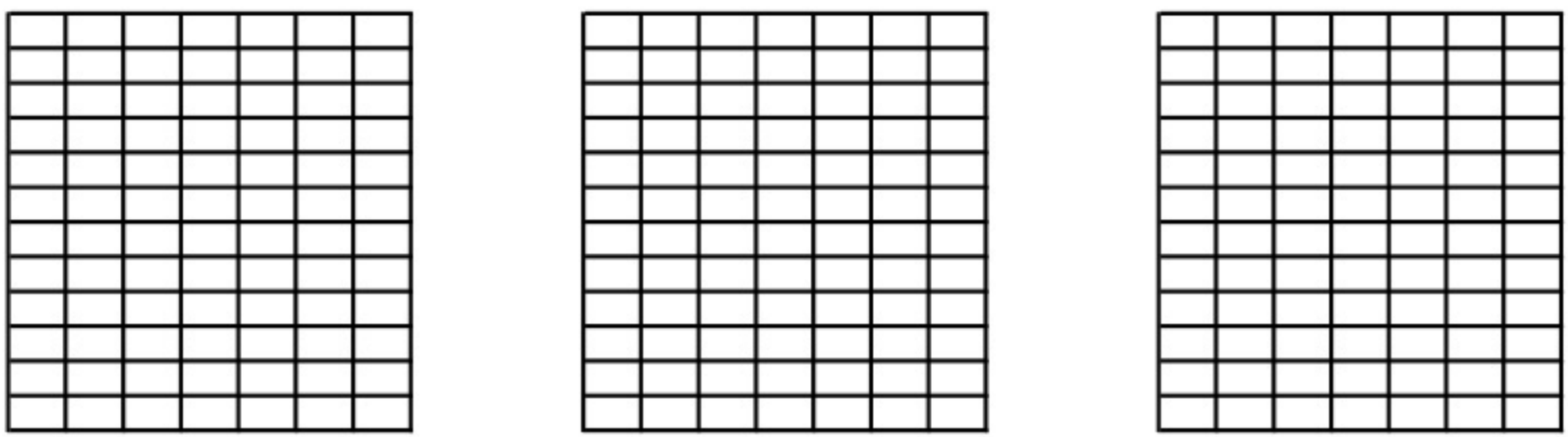


Reference Signals and Channel Estimation

- In order to make use of both amplitude and phase information carried by OFDMA symbols, channel estimation is required.
- For UE moving at 500 km/h, the Doppler shift is fd=950Hz. Reference signals need to be presented every 1/(2*fd) = 0.5 ms. This implies two reference symbols per slot.
- Every Resource Block (RB) contains 4 reference symbols for one antenna, and 8 reference symbols for two antennas.

Reference Signals and Channel Estimation

- Reference Signals (RSs) provide phase reference for demodulating PDSCH.
- Reference Signals (RSs) are also used for power measurements.



One antenna port Two antenna ports Four antenna ports

Downlink Physical Channels Mapping

- Physical Broadcast Channel (PBCH):
  - Detectable without prior knowledge of system bandwidth; by mapping PBCH only to the central 72 sub-carriers regardless of system bandwidth.
  - Low system overhead: MIB is 14 bits only.
  - Reliable reception: MIB is coded at a very low code-rate.
  - MIB is spread over 40ms interval (four frames).

Downlink Physical Channels Mapping

Type of physcial channel or signal contained in RE

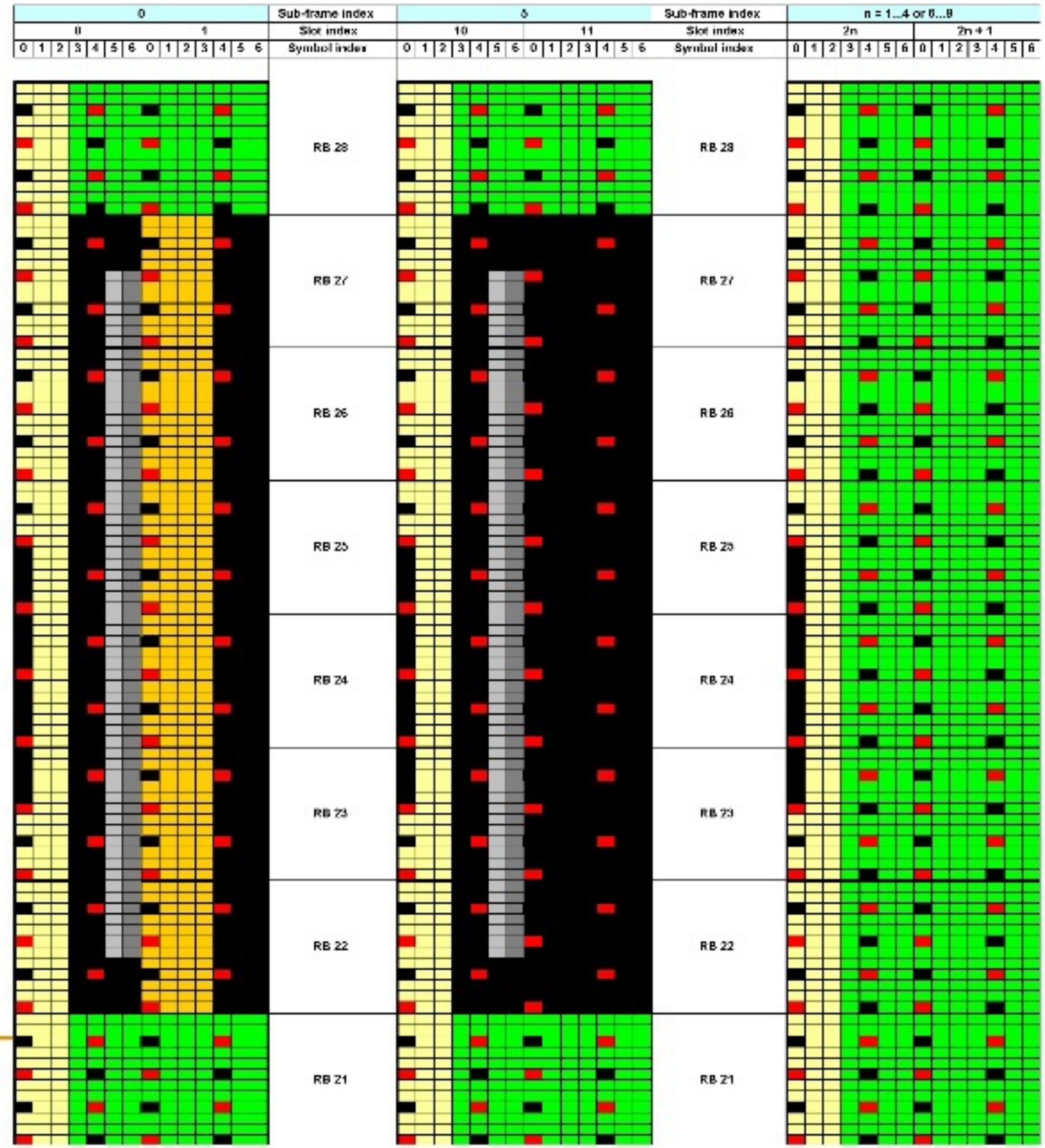
- RS0
- RS1
- PCFICH, PHICH and PDCCH
- PDSCH
- PBCH
- PSS
- SSS
- No signal (i.e., 0) transmitted on this RE

- Unused PDSCH
- PCFICH (illustrates one of four resource element groups)
- PHICH (illustrates one of 7 PHICH groups)

Notes:

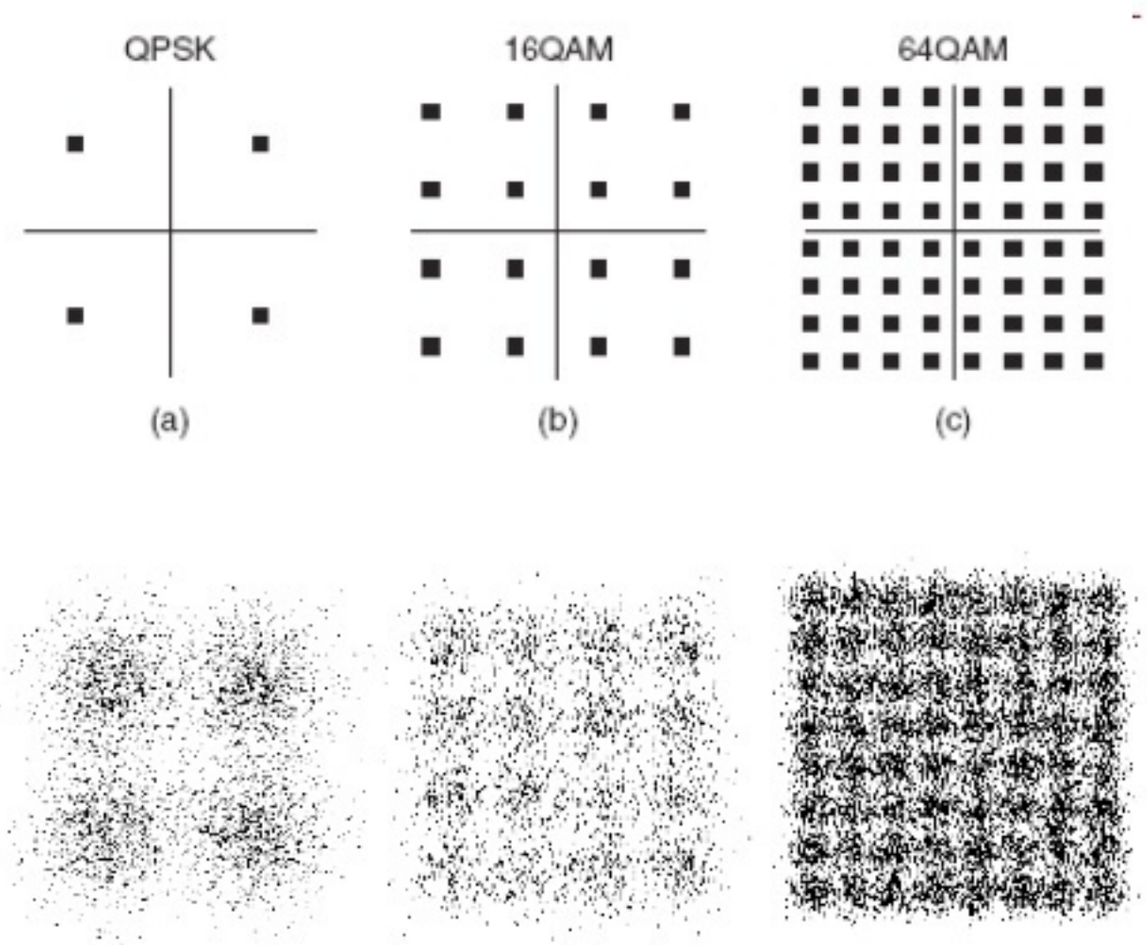
Shown with 3 OFDM-symbols for PDCCH

Format for RB 0-20 and 28-49 are not shown but are identical to RB 28



Constellations of Modulation Schemes

- Modulation vary from two bits per symbol using QPSK to six bits per symbol using 64QAM.
- UE looks for PDCCH to find which DL RB is allocated to it.



Layer 1 Downlink Physical Control Channels

- Physical Control Format Indicator (PCFICH)
  - It indicates number of symbols used for PDCCH.
- Physical Downlink Control Channel (PDCCH)
  - Resource block grant to UEs.
  - Modulation and coding scheme for RBs.
- Physical Hybrid ARQ Indicator Channel (PHICH)
  - Carries HARQ ACK/NACK which indicates whether eNB has correctly received PUSCH.

Channel Coding and Link Adaptation

- Channel coding enhances robustness of transmitted bits by adding Cyclic Redundancy Check (CRC), Turbo encoding, interleaving, and bit repetition.
- Channel Quality Indicator (CQI)
  - Periodically reported by UE in PUCCH.
  - A combination of Block Error Rate (BLER), Signal to Interference and Noise Ratio (SINR), and UE receiver capability.
  - CQI values from 0 to 15. 0 lowest and 15 highest.

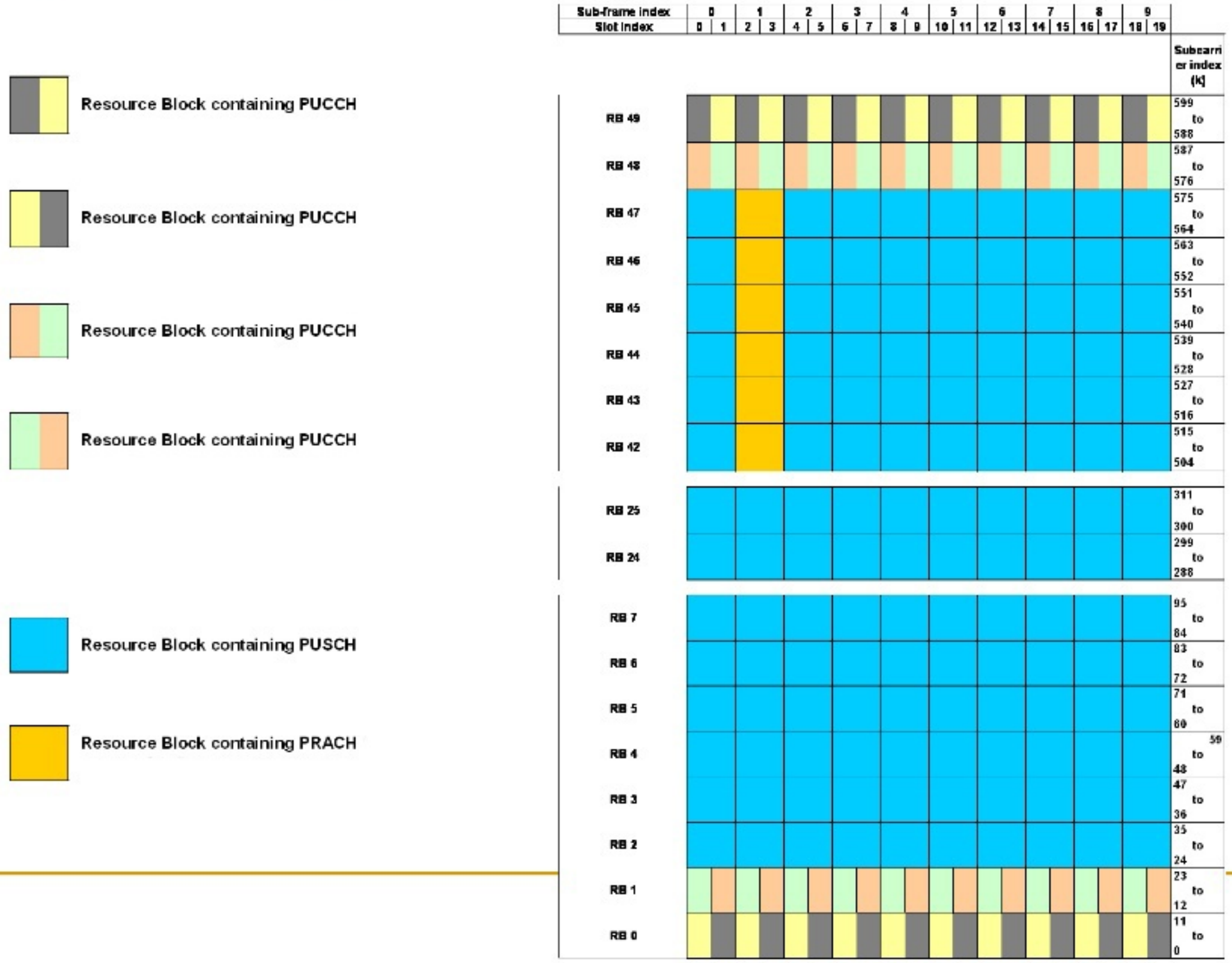
Channel Quality Indicator Mapping

CQI Index	Modulation	Code Rate	Efficiency (bit/symbol)
0	No transmission	-	-
1	QPSK	0.076	0.1523
2	QPSK	0.12	0.2344
3	QPSK	0.19	0.3770
4	QPSK	0.3	0.6016
5	QPSK	0.44	0.8770
6	QPSK	0.59	1.1758
7	16QAM	0.37	1.4766
8	16QAM	0.48	1.9141
9	16QAM	0.6	2.4063
10	64QAM	0.45	2.7305
11	64QAM	0.55	3.3223
12	64QAM	0.65	3.9023
13	64QAM	0.75	4.5234
14	64QAM	0.85	5.1152
15	64QAM	0.93	5.5547

LTE Measurements

- Reference Signal Received Power (RSRP)
  - Power average of Reference Signals (RS) for one RB.
  - Used to rank candidate cells for handover and cell reselection.
- Received Signal Strength Indicator (RSSI)
  - Total received wideband power including interference, co-channel cells, and thermal noise.
  - Changes according to cell throughput. RSSI is not reported.
- Reference Signal Received Quality (RSRQ)
  - RSRQ = N * RSRP / RSSI where N=no. of RBs.
  - Used to rank candidate cells according to their signal strength.

Uplink Physical Channel Mapping

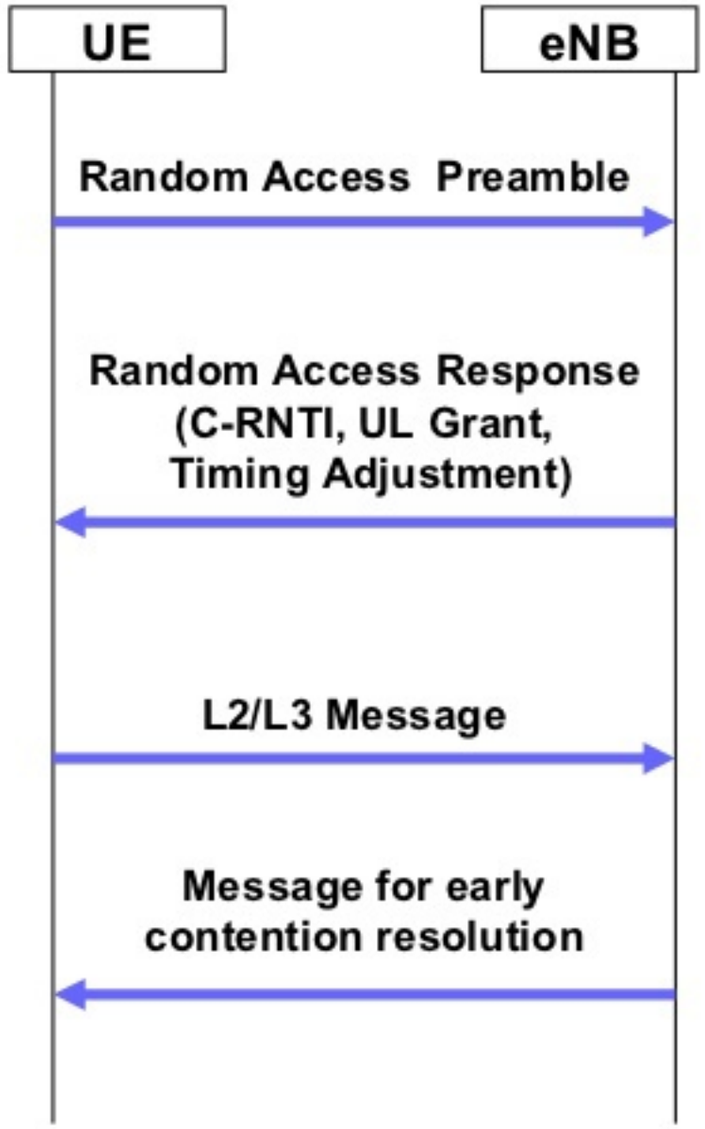


Layer 1 Uplink Physical Control Channels

- Physical Uplink Control Channel (PUCCH)
  - UL HARQ ACK/NACK for downlink data packets.
  - Channel Quality Indicator (CQI) reports.
  - MIMO feedback and Rank Indicator (RI).
  - Scheduling Requests (SRs) for uplink transmission.
- Physical Random Access Channel (PRACH)
  - Initial network access and uplink time sync.
  - Request to send new uplink data or control.
  - Handing over from current cell to target cell.

Random Access Procedure

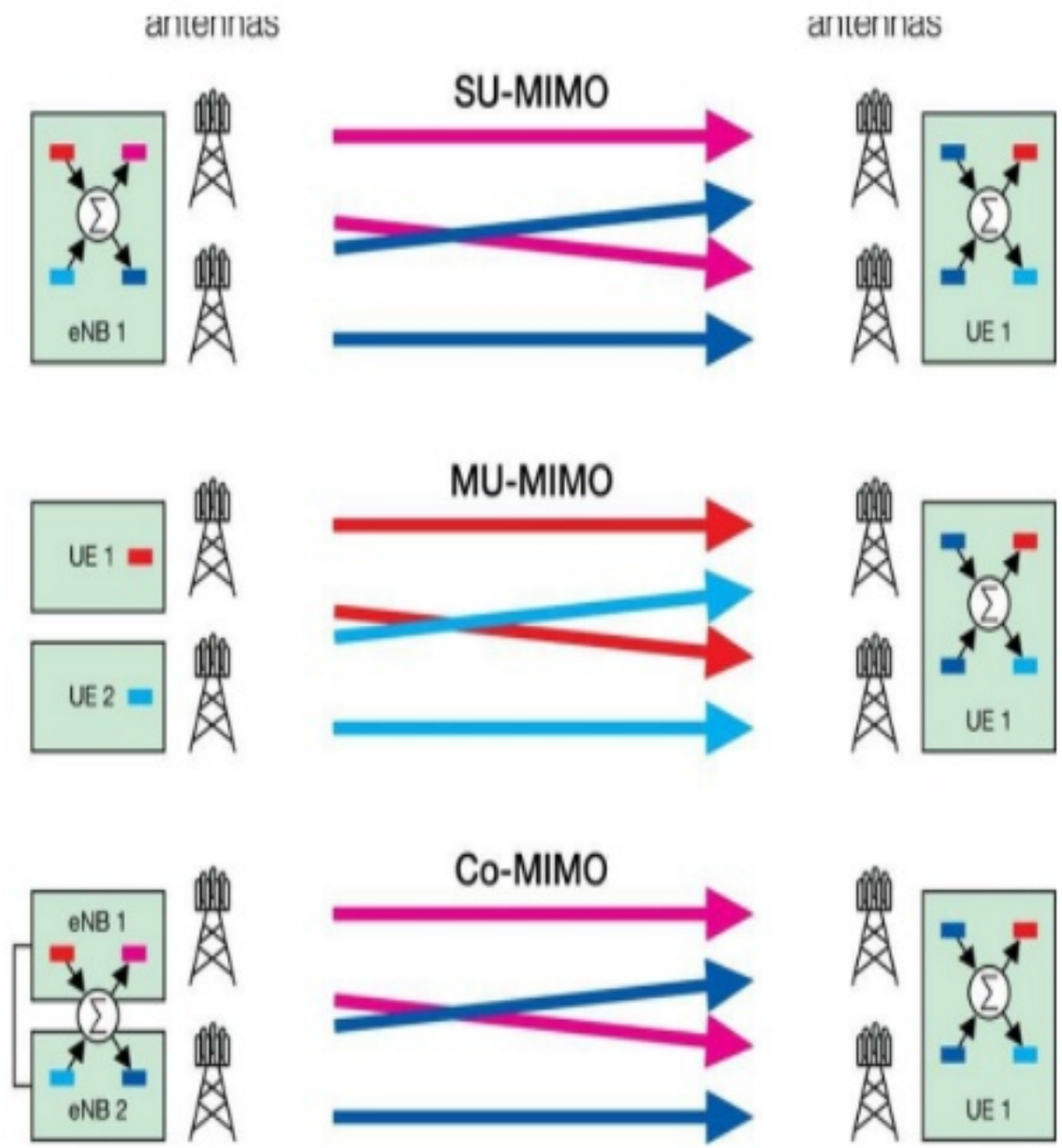
- Contention based random access procedure.
  1. Preamble transmission (one of 64 preambles).
  2. Random access response sent from eNB on PDSCH addressed with Cell Radio Network Temporary Identifier (C-RNTI).
  3. Sending actual L3 message (i.e., RRC connection request) on PUSCH. HARQ enabled.
  4. Contention Resolution Message.

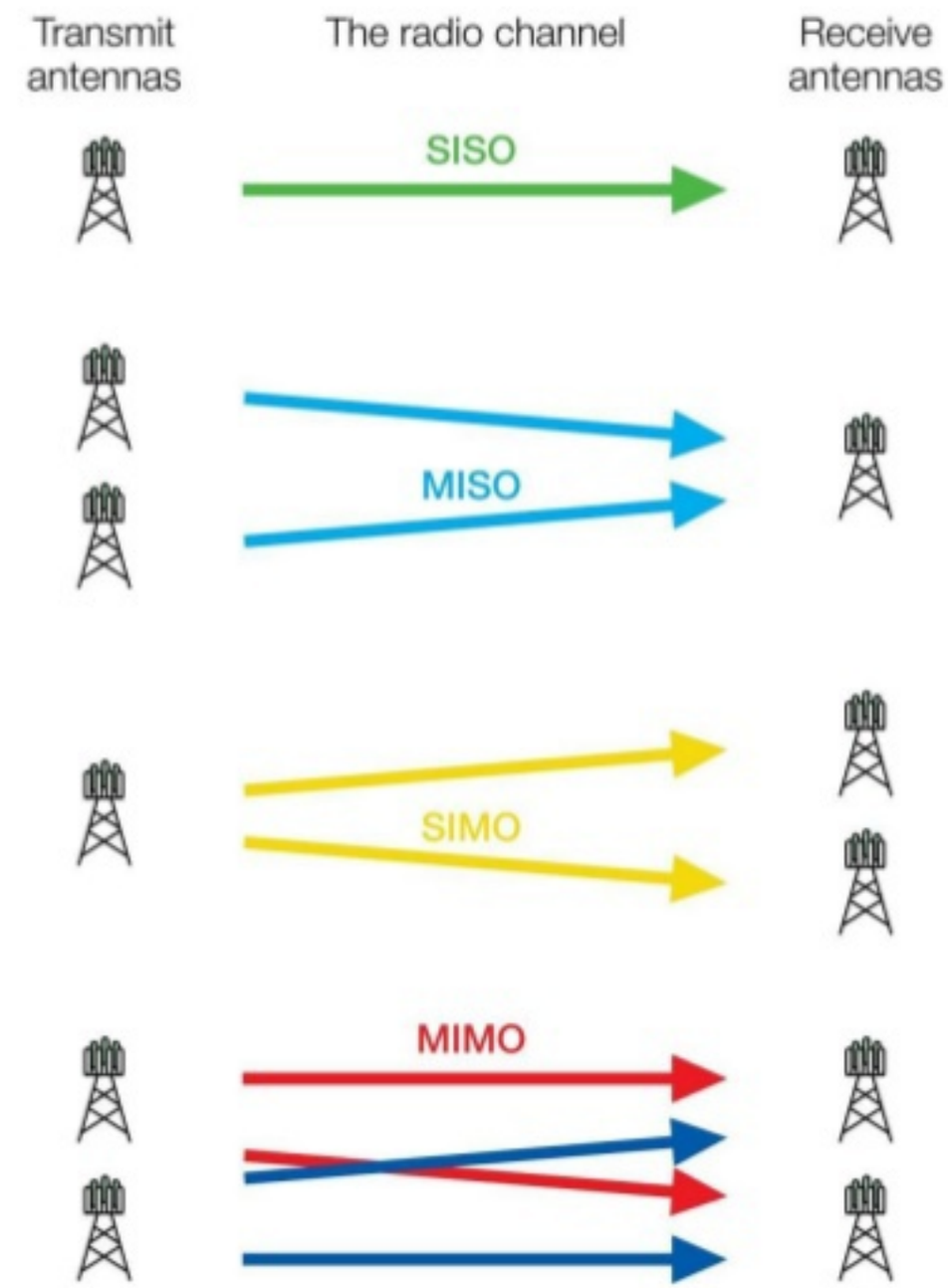


Multiple Antenna Techniques

- Multiple antennas can be configured in terms of number and configuration as the following:
  - Single-Input Single-Output (SISO).
  - Single-Input Multiple-Output (SIMO).
  - Multiple-Input Single-Output (MISO).
  - Single-User Multiple-Input Multiple-Output (SU-MIMO).
  - Multi-User Multiple-Input Multiple-Output (MU-MIMO).

Multiple Antenna Techniques

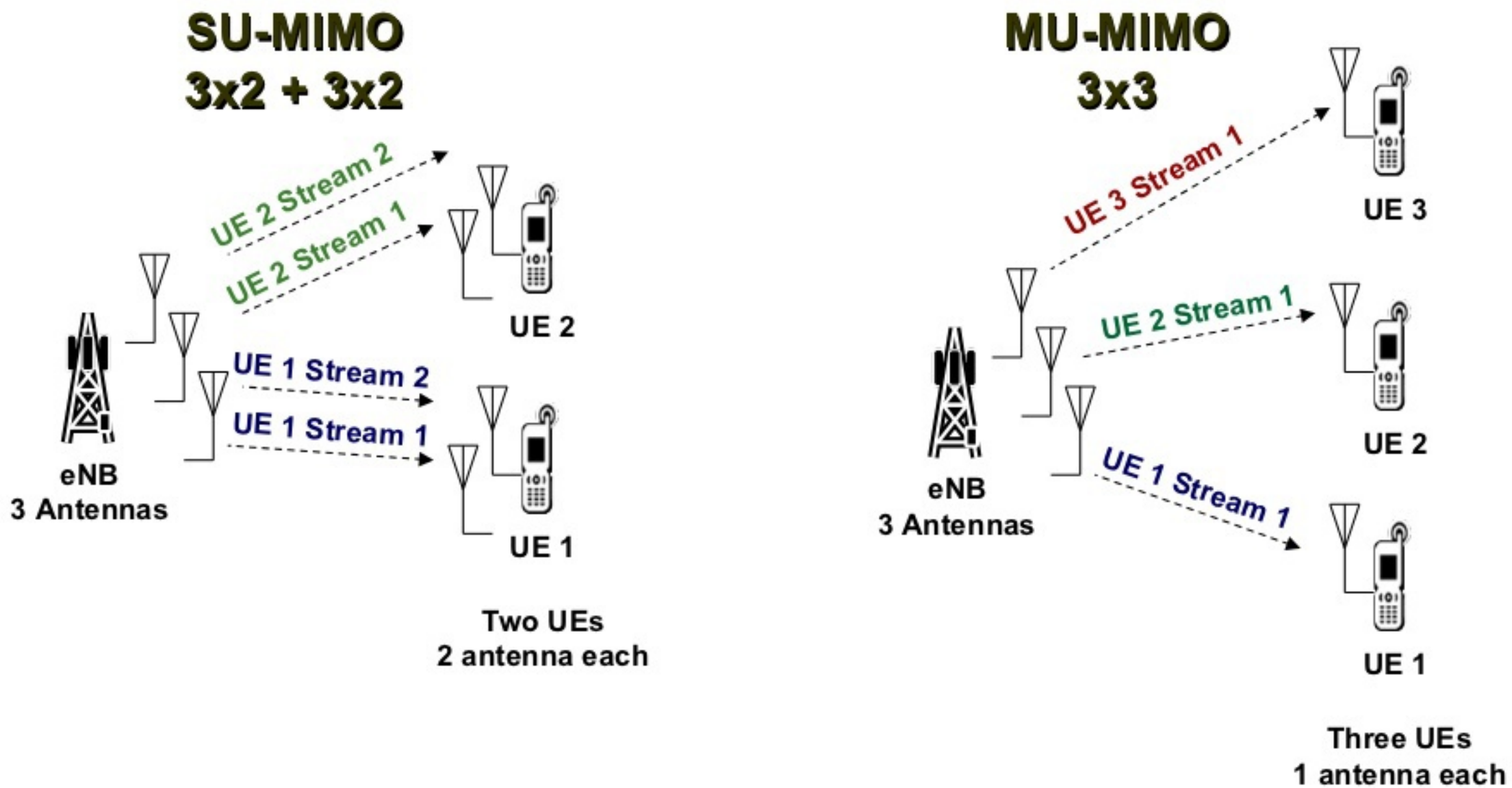




Advantages of Multiple Antennas

- Three advantages are possible with Multiple Antennas:
  - Diversity Gain: mitigating multi-path fading.
  - Array Gain: Beamforming; maximizing SNR for UEs.
  - Spatial Multiplexing: multiple data streams; higher throughput.
- Single-User vs Multi-user MIMO:
  - SU-MIMO multiplexes N eNB antennas to M UE antennas, while MU-MIMO multiplexes N eNB antennas to M antennas * no. of active UEs in cell.
  - SU-MIMO requires at least two antennas at UE while MU-MIMO can have one antenna for UE; low-cost UEs benefit from MU-MIMO.
  - SU-MIMO requires rich multi-path propagation for de-correlation between antennas, while in MU-MIMO de-correlation is natural due to the obvious large separation between UEs

SU-MIMO vs MU-MIMO



Beamforming Schemes

- Closed-loop rank 1 precoding:
  - UE feeds channel information back to eNB to indicate suitable precoding to apply for the beamforming operation.
- UE-specific Reference Symbols (RSs):
  - UE does not feed back any precoding information. eNB deduce this information using Direction Of Arrival (DOA) estimation from the uplink.
  - eNB is responsible for directing the beam.

LTE Transmission Modes

- LTE transmission modes:
  - Mode 1: Transmission from a single eNB antenna port.
  - Mode 2: Transmit diversity.
  - Mode 3: Open-loop spatial multiplexing.
  - Mode 4: Closed-loop spatial multiplexing.
  - Mode 5: Multi-user Multiple-Input Multiple-Output (MIMO).
  - Mode 6: Closed-loop rank-1 precoding.
  - Mode 7: Transmission using UE-specific reference signals.
- Transmission Mode is broadcasted in SIB.

Further Readings

- 3GPP Technical Specification 36.321, “Medium Access Control (MAC) protocol specification” (Release 8) www.3gpp.org.
- 3GPP Technical Specification 36.201, “LTE Physical layer; General description” (Release 8) www.3gpp.org.
- 3GPP Technical Specification 36.212, “Multiplexing and Channel Coding (FDD)” (Release 8) www.3gpp.org.
- 3GPP Technical Specification 36.213, “Physical Layer Procedures” (Release 8) www.3gpp.org.

LTE

3GPP Standard Perspective

Chapter 5 – SAE and the Evolved Packet Core

Muhannad Aulama

Contents of Chapter 5

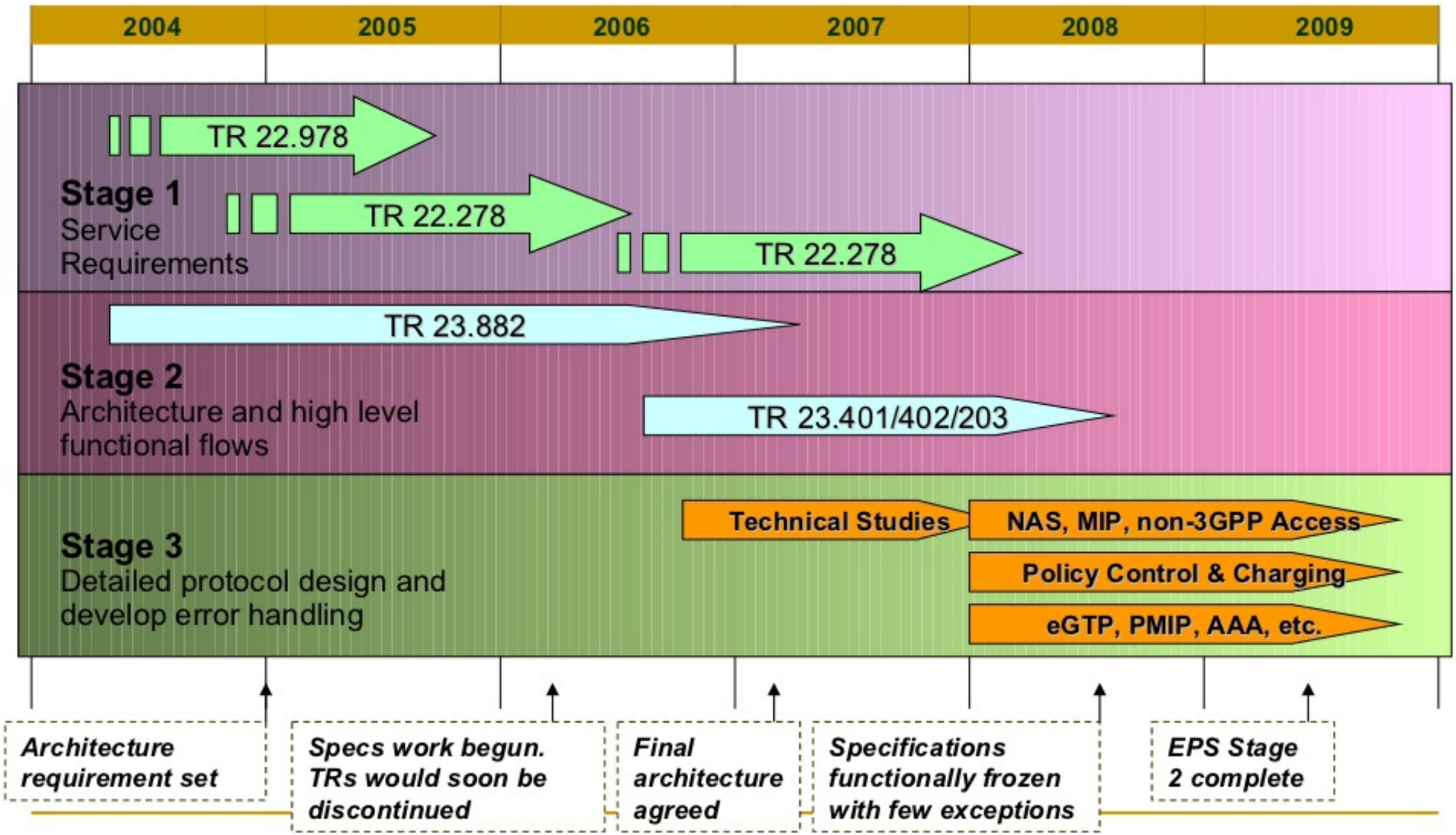
- Introduction.
- History
- EPC Scope.
- EPC Architecture.
- EPC Interfaces.
- Key Protocols in EPC.
- Voice Services in EPC.
- PDN Connectivity in EPC.
- Transport Network in EPC.
- QoS in EPC.
- User Plane QoS handling.
- GTP for EPS Bearers.
- GTP Protocol Format and Flow.
- Mobility Management in EPC.
- Nodes Identifiers in EPC.
- Subscriber Identifiers in EPS.
- Diameter.
- Security.
- HSS User Profile.
- Policy and Charging Control (PCC).
- Elements of PCC Rule.
- Charging.
- Charging Data Records (CDRs) Contents.
- Selection Function.
- Further Readings.

Introduction

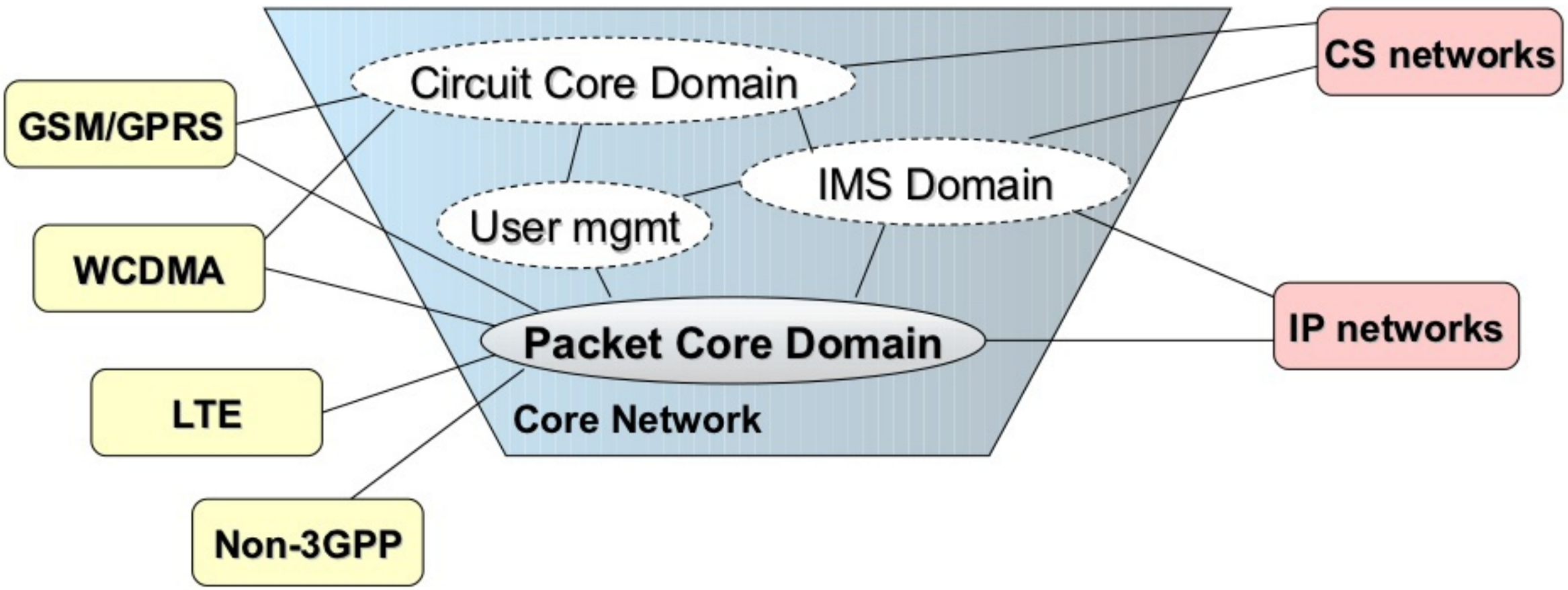
- System Architecture Evolution (SAE) is the name of a 3GPP standardization work item responsible for the evolution of the packet core network (EPC).
- 3GPP the owner and lead organization initiating SAE, along with 3GPP2, IETF*, WiMAX Forum, and OMA** collaborate for the development of SAE.
- Goal is to have a simplified all-IP architecture providing support for multiple radio access networks including different radio standards.

IETF: Internet Engineering Task Force
****OMA: Open Mobile Alliance***

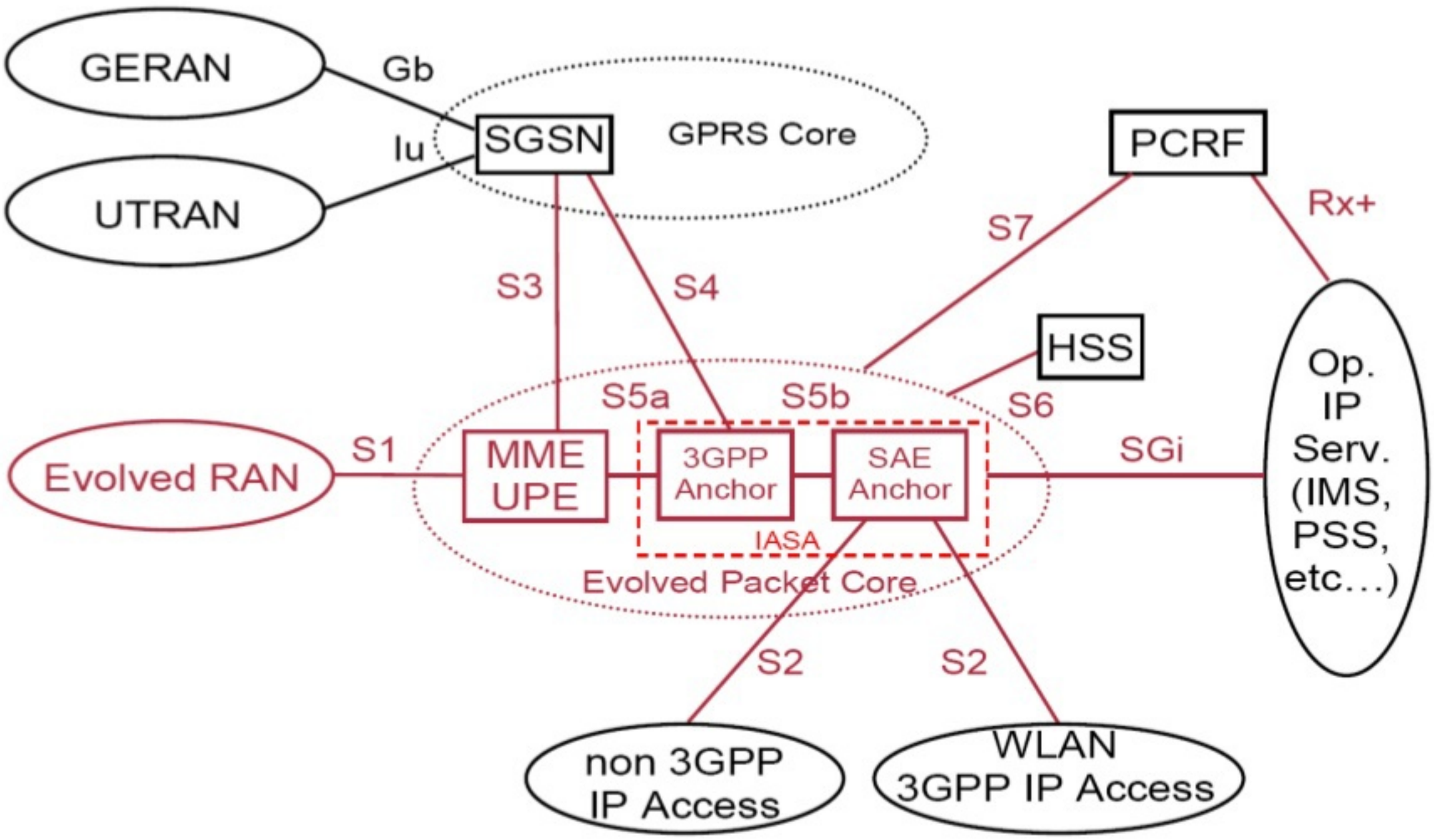
History


2004
2005
2006
2007
2008
2009
TR 22.978
Stage 1
Service
Requirements
TR 22.278
TR 22.278
TR 23.882
Stage 2
Architecture and high level
functional flows
TR 23.401/402/203
Stage 3
Detailed protocol design and
develop error handling
Technical Studies
NAS, MIP, non-3GPP Access
Policy Control & Charging
eGTP, PMIP, AAA, etc.
Architecture requirement set
Specs work begun. TRs would soon be discontinued
Final architecture agreed
Specifications functionally frozen with few exceptions
EPS Stage 2 complete

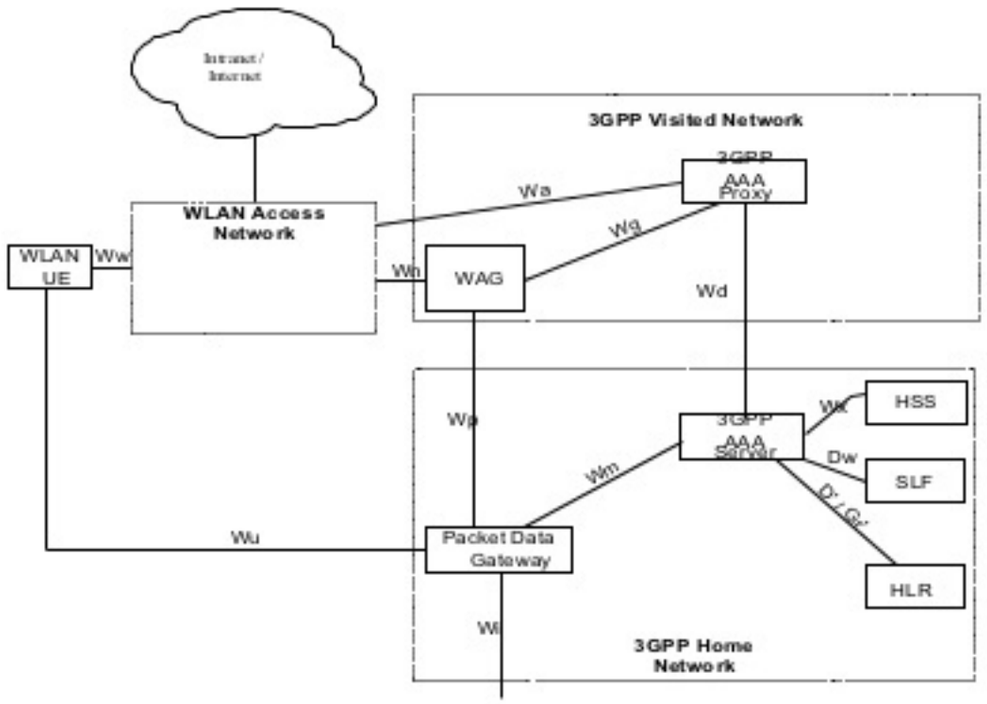
EPC Scope

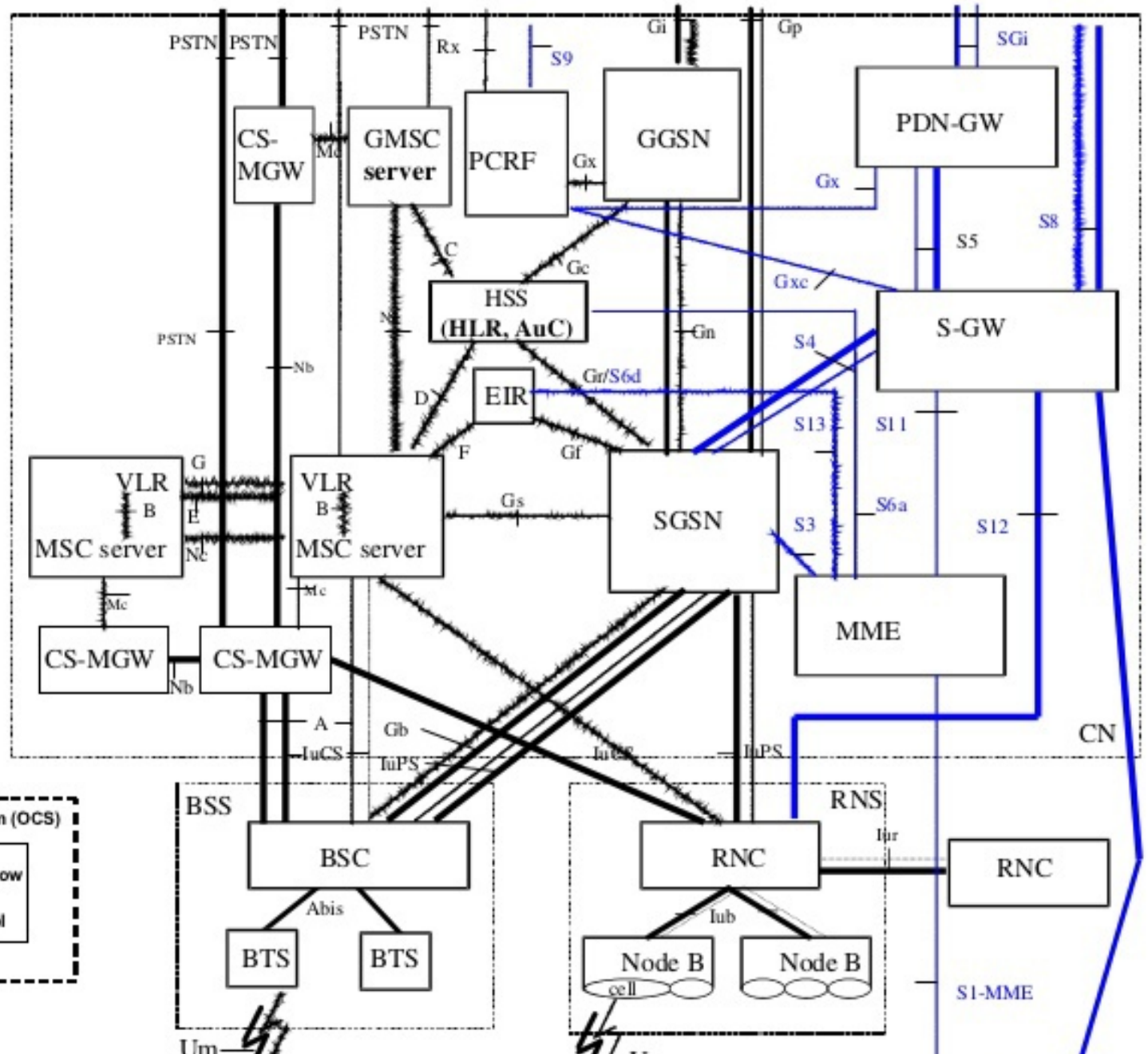

Circuit Core Domain
IMS Domain
User mgmt
Packet Core Domain
Core Network
GSM/GPRS
WCDMA
LTE
Non-3GPP
CS networks
IP networks

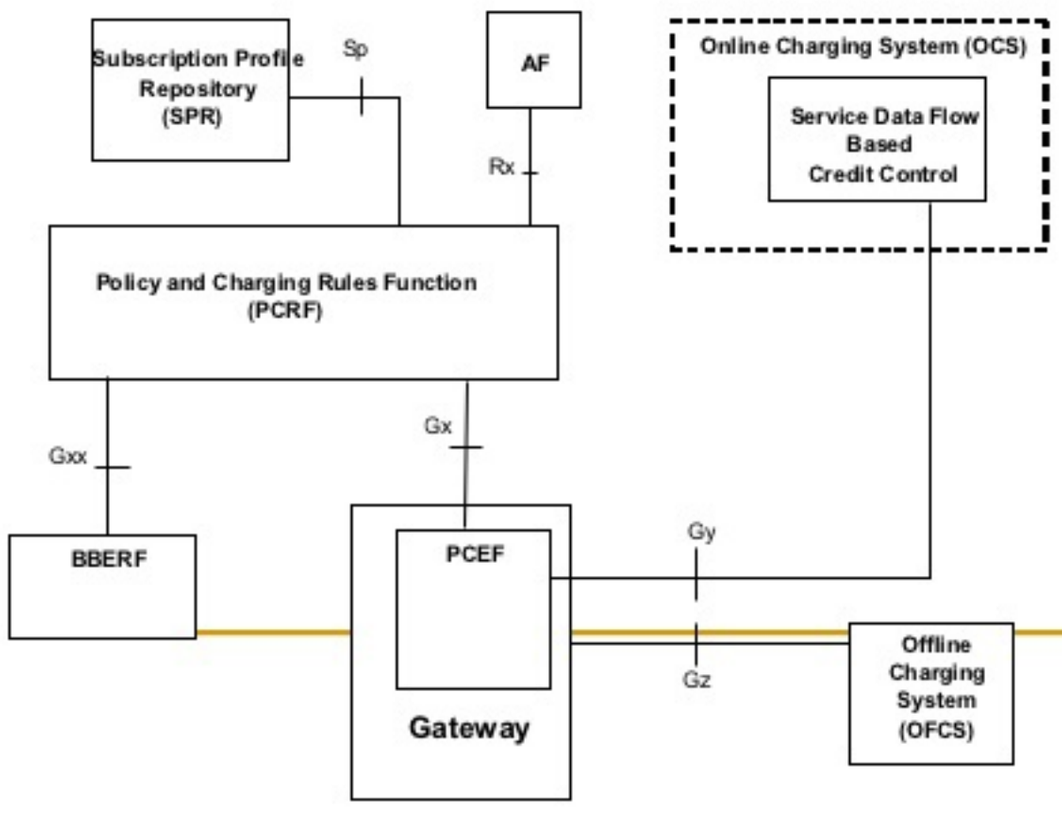
EPC Architecture



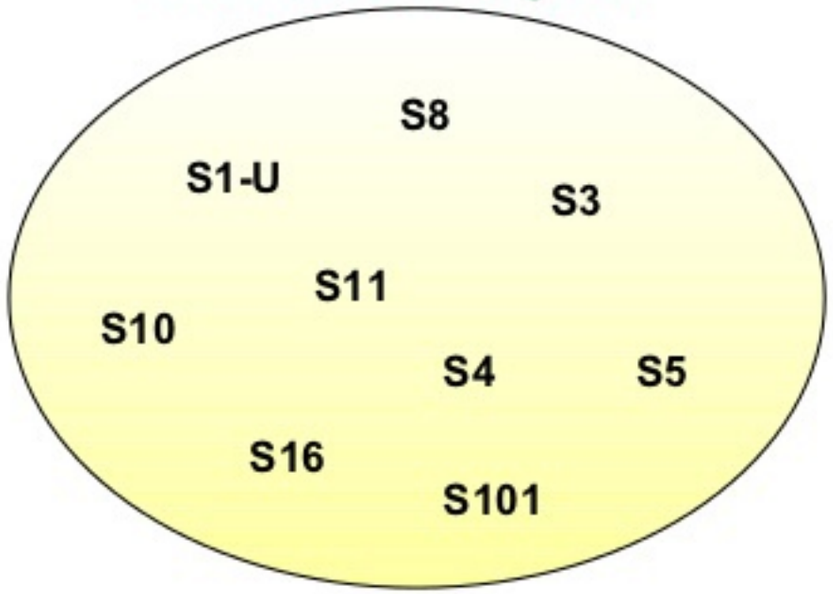
EPC Interfaces

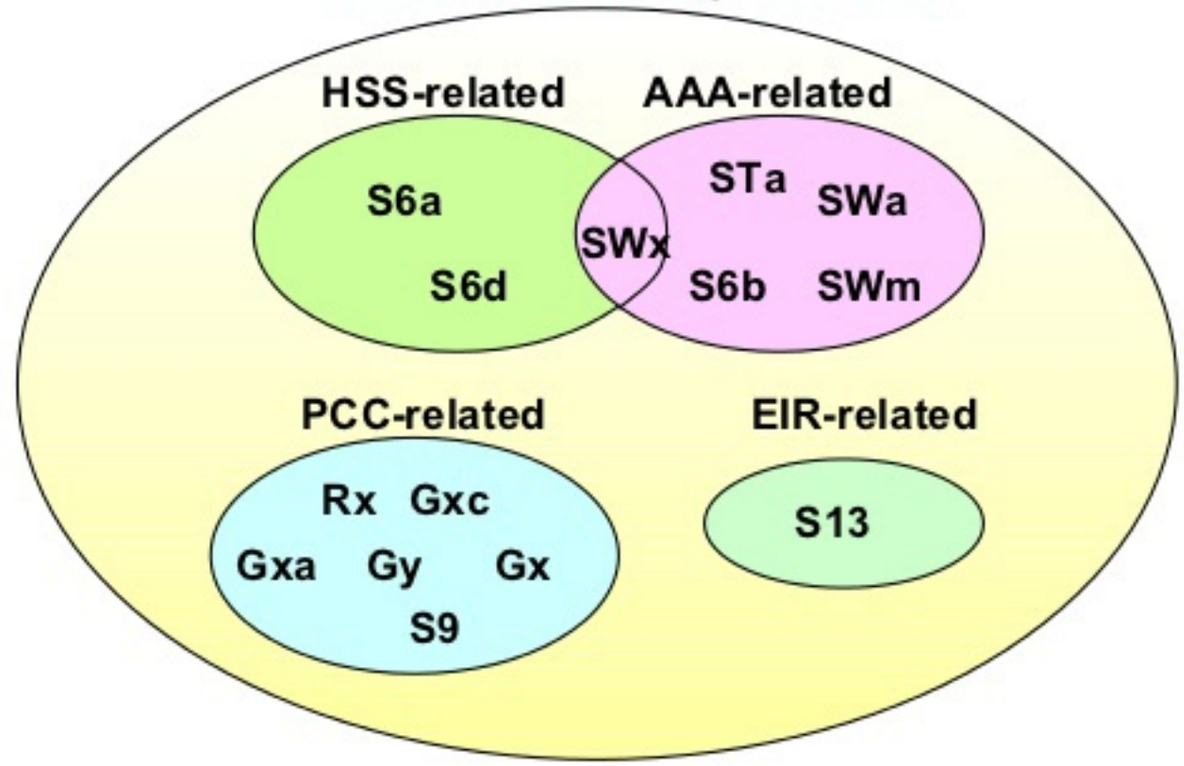


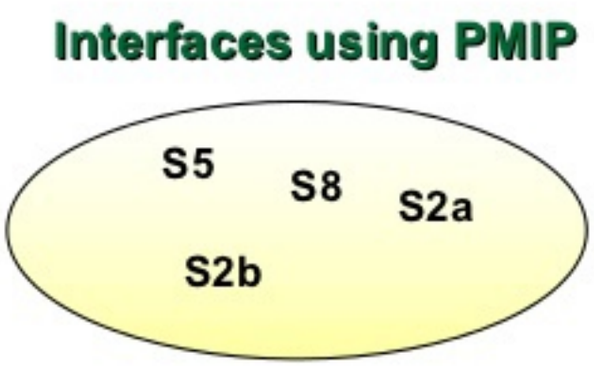


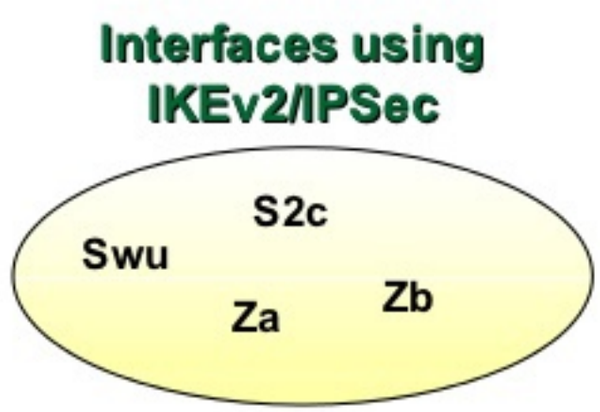


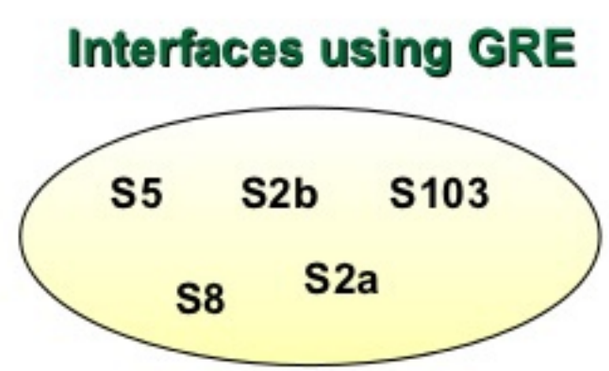
Key Protocols in EPC





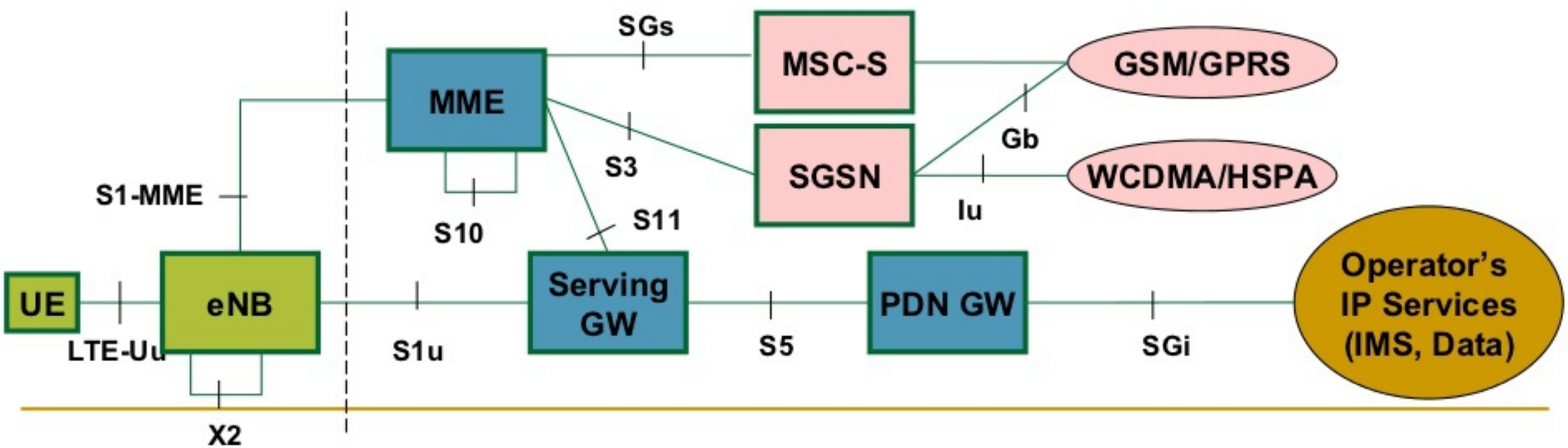






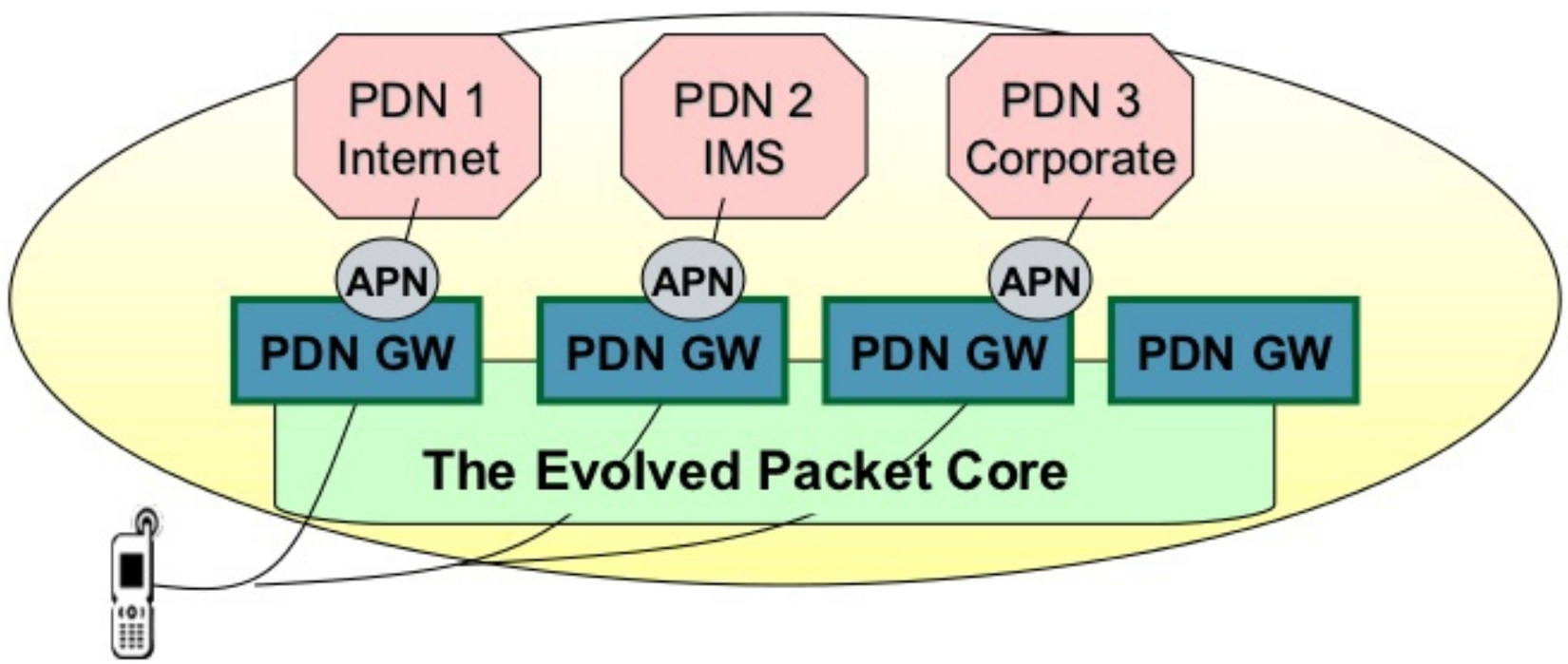
Voice Services in EPC

1. Multimedia Telephony (MMTel)
   - IMS or VOIP over LTE.
   - Can be handed over to WCDMA/non-3GPP access networks. (S3 for 3G, S101 for CDMA).
2. Circuit Switched Fallback (CSFB)
   - Supported through signaling over SGs interface between MME and MSC. No need for IMS deployment.
   - User leaves LTE to perform voice call over 2G/3G.



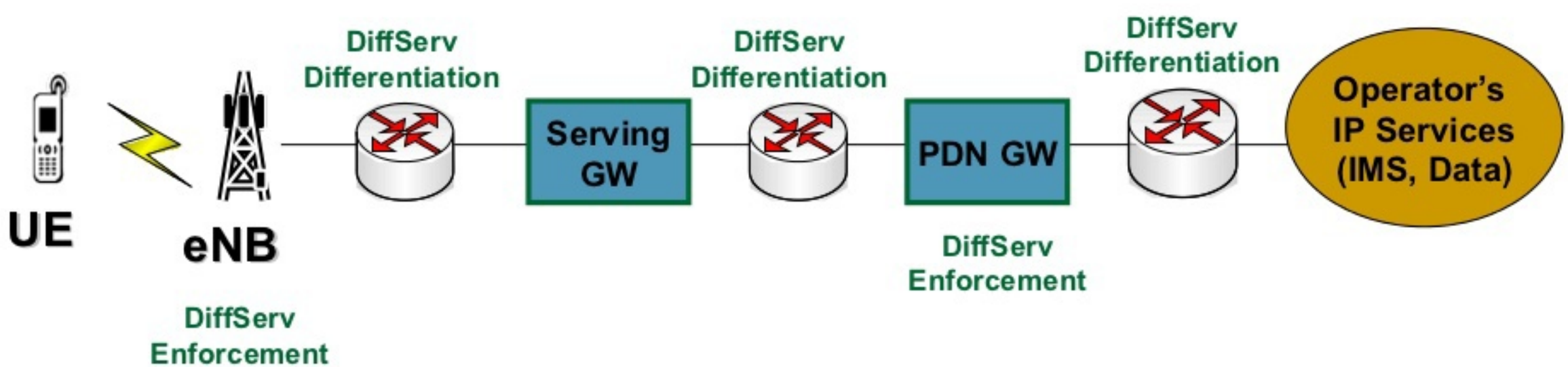
PDN Connectivity in EPC

- UE can have multiple PDN connections simultaneously, each having unique IP address, end-to-end bearer, QoS, etc.



Transport Network in EPC

- IP transport using MPLS, Ethernet, Wireless P2P, etc.
- Traffic differentiation in transport network is based on Differentiated Services (DiffServ).
- DiffServ is enforced at eNB and PGW.
- DiffServ provides up to 64 QoS classes in IP TOS field.



QoS in EPC

- Each end-to-end EPC bearer has QoS parameters describing the properties of bearer's transport channel.
- Data is filtered at PGW and UE for appropriate EPC bearer using filtering attributes (TFTs).

Packet Filter Attribute
Remote address and subnet mask
Protocol number (IPv4) / next header (IPv6)
Local port range
Remote port range
IPSec Security Parameter Index (SPI)
Type of Service (TOS) (IPv4) / Traffic Class (IPv6)
Flow Label (IPv6)

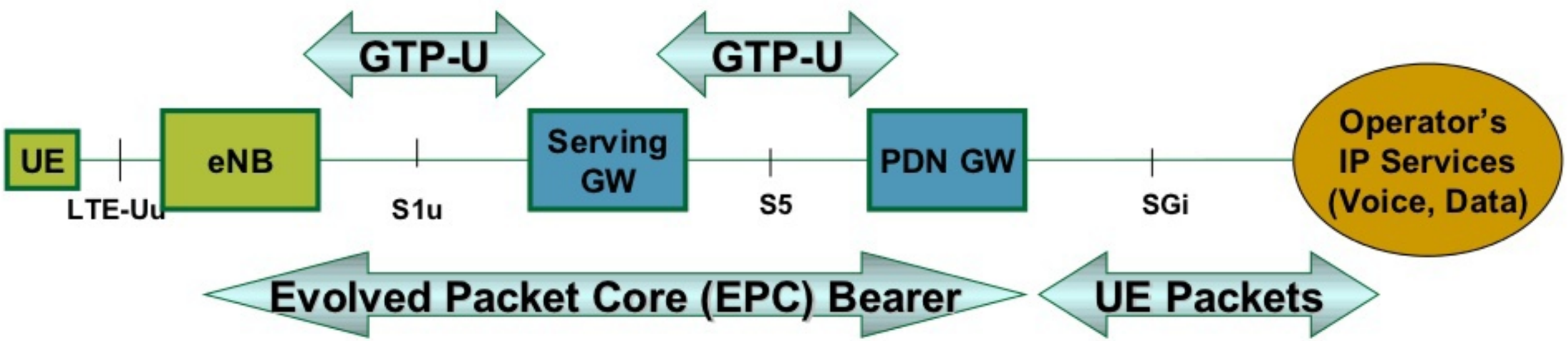
QoS Attribute
QoS Class Id (QCI); a pointer for QoS profile
Allocation and Retention Priority (ARP); priority for resource allocation contention
Maximum Bit Rate (MBR)
Guaranteed Bit Rate (GBR)
Packet Delay (in millisecond)
Packet error loss rate (e.g. 10^{-2})

User Plane QoS Handling

	UE	eNB	Transport Network	PDN GW
Packet Filtering	X (Uplink)			X (Downlink)
GBR/ARP Admission		X		X
ARP Pre-emption		X		X
Rate Policing		X		X
Queue Management	X	X		
Uplink + Downlink Scheduling		X		
Configuring Layer 1/2 Protocols		X		
Map QCI to DSCP		X		X
Queue Management			X	
Uplink + Downlink Scheduling			X	

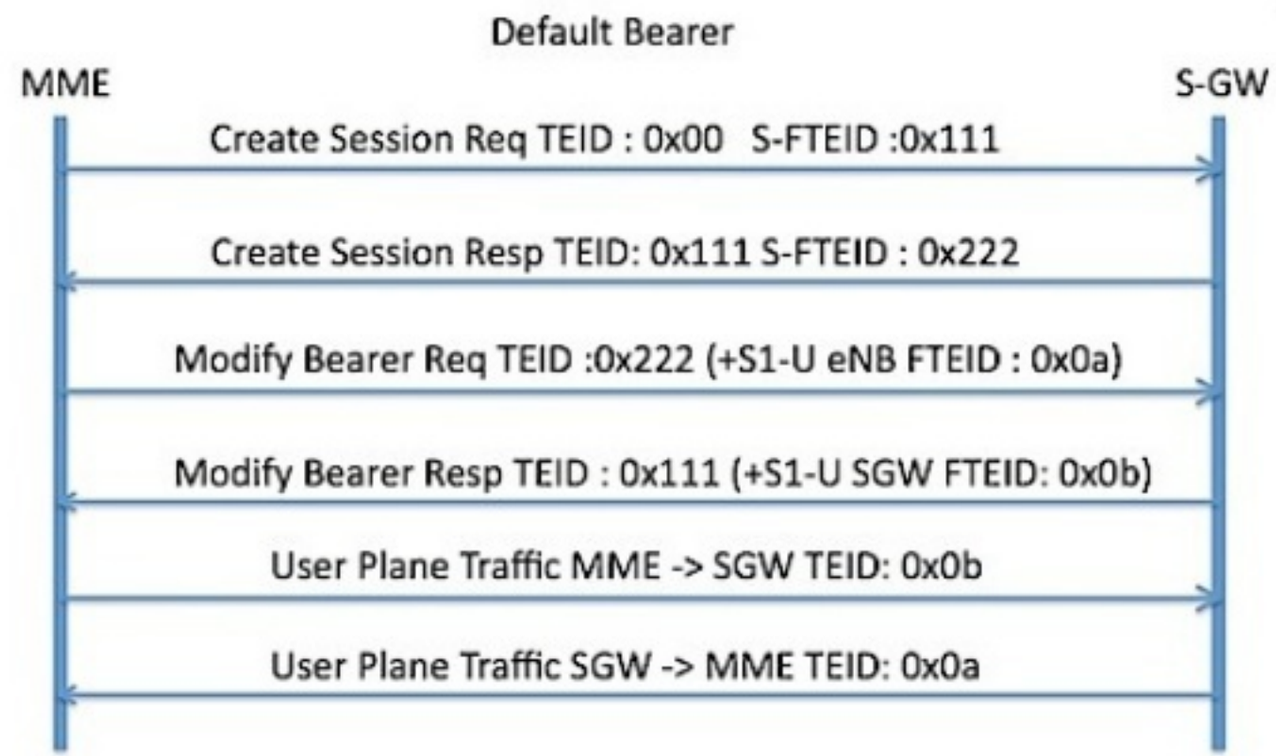
GTP for EPS Bearers

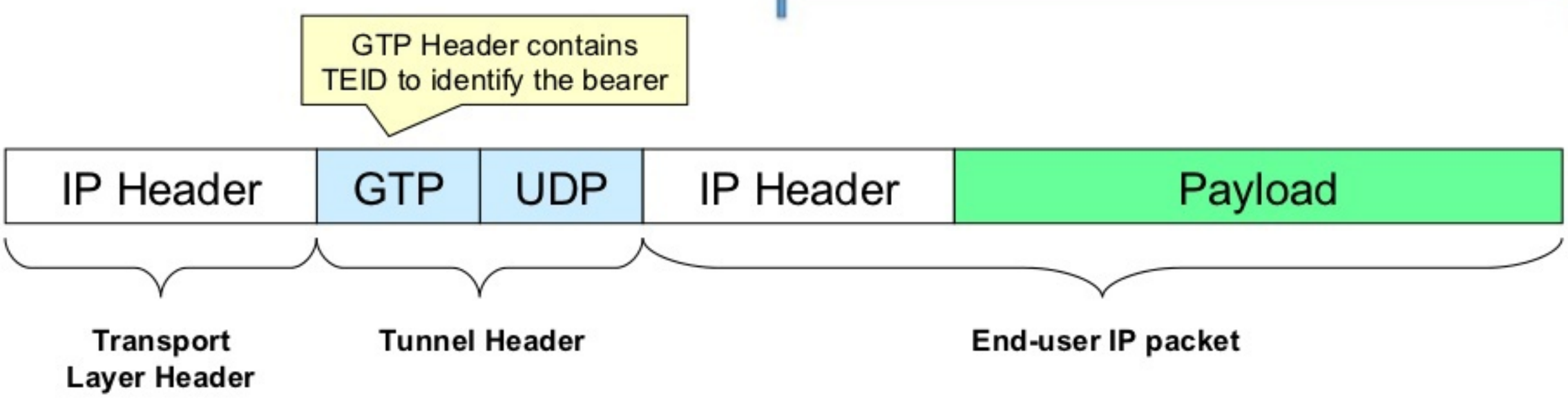
- All EPS user-plane bearers are established using GPRS Tunneling Protocol (GTP) or Proxy Mobile IP (PMIP).
- GTP User Plane (GTP-U) information (e.g., TEID, end point IP) are set initially during GTP Control (GTP-C) tunnel creation procedure.



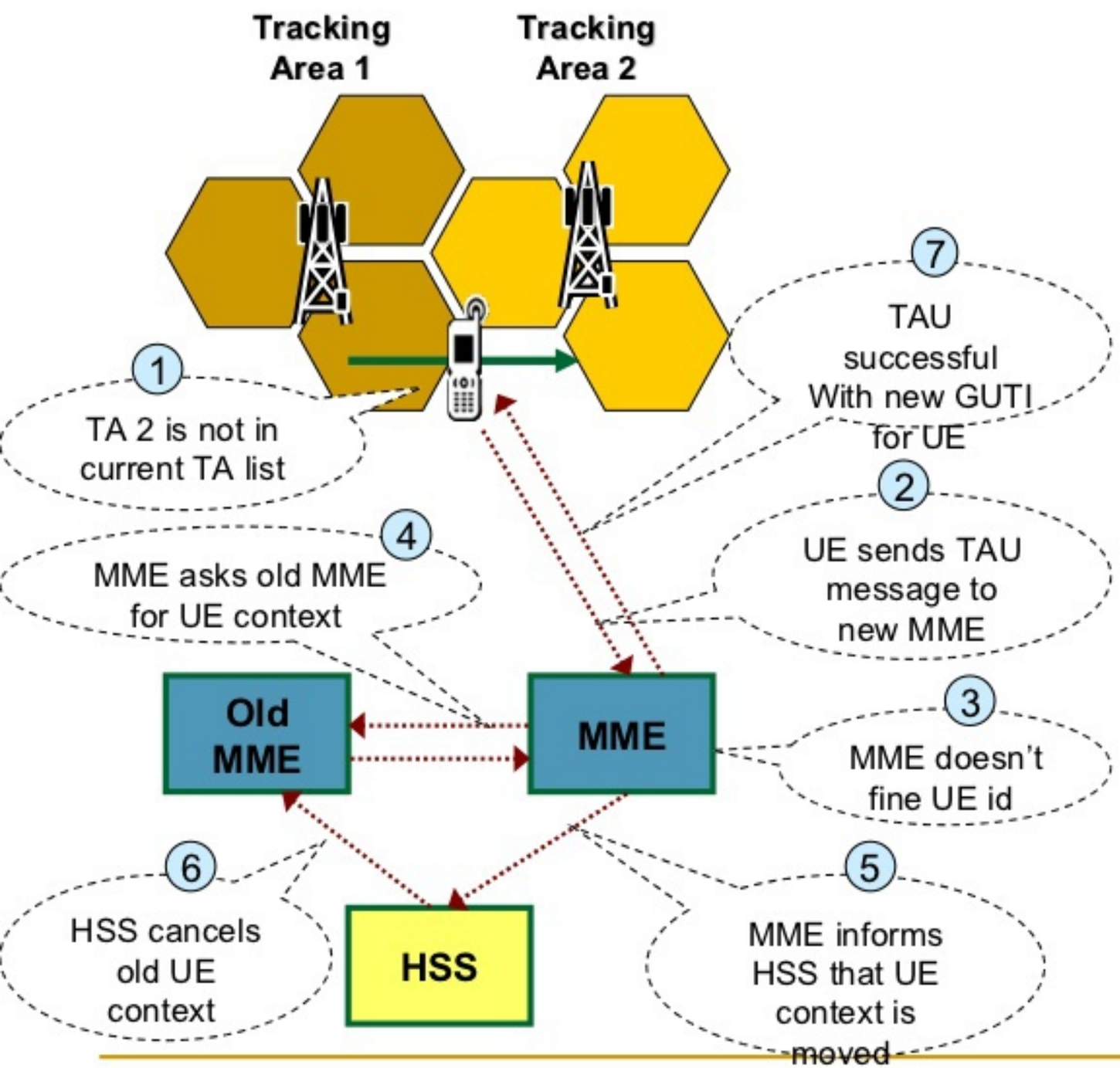
GTP Protocol Format and Flow

- "Create" messages to negotiate peers TEID.
- "Modify" messages to negotiate GTP-U TEIDs, i.e., those for eNB and SGW

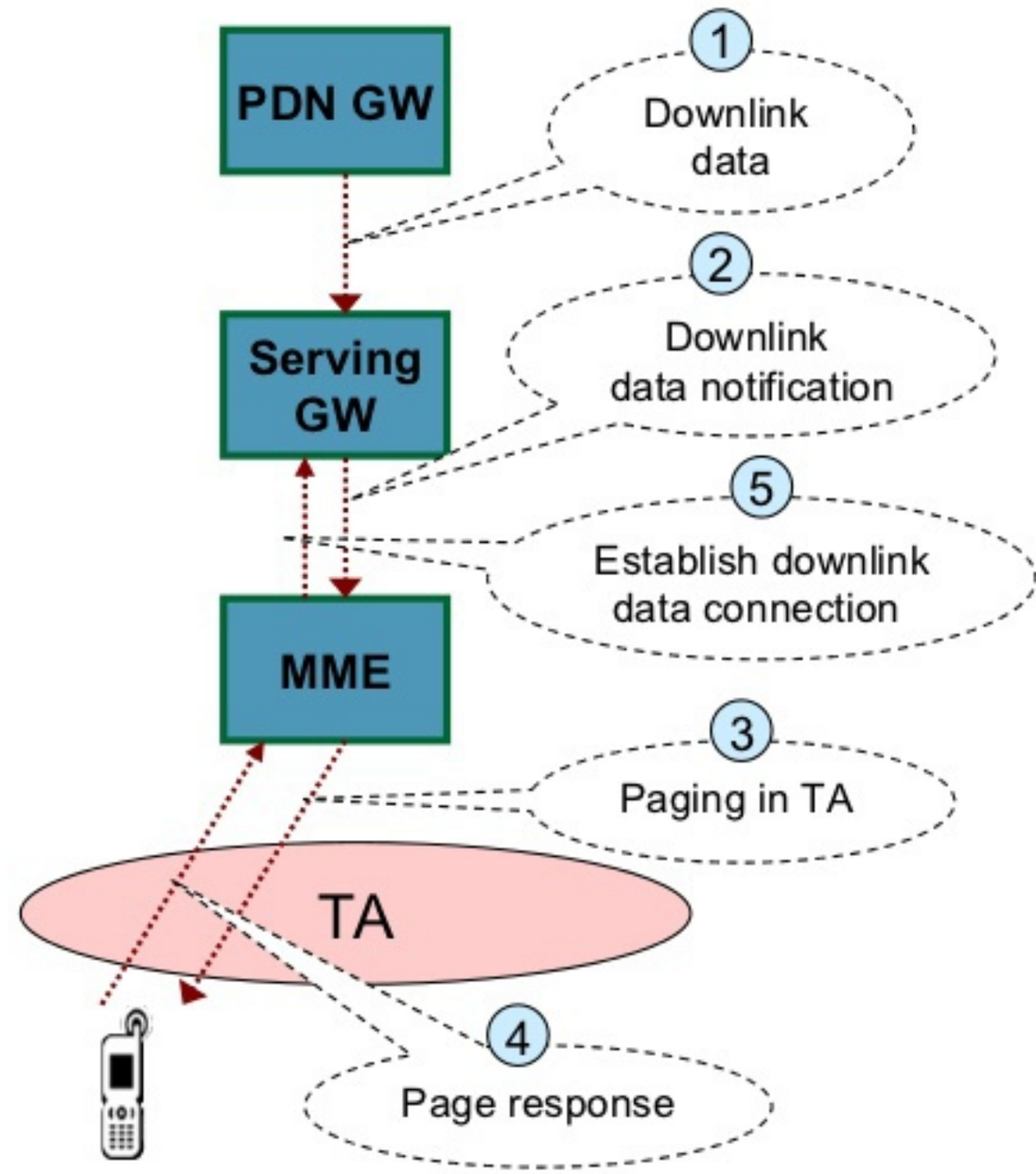




Mobility Management in EPC

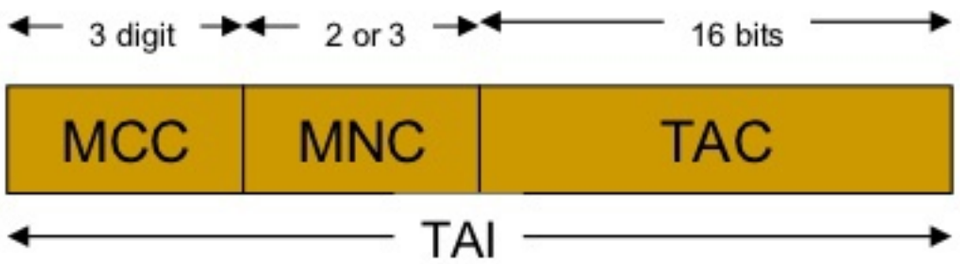


Tracking Area Update



Paging

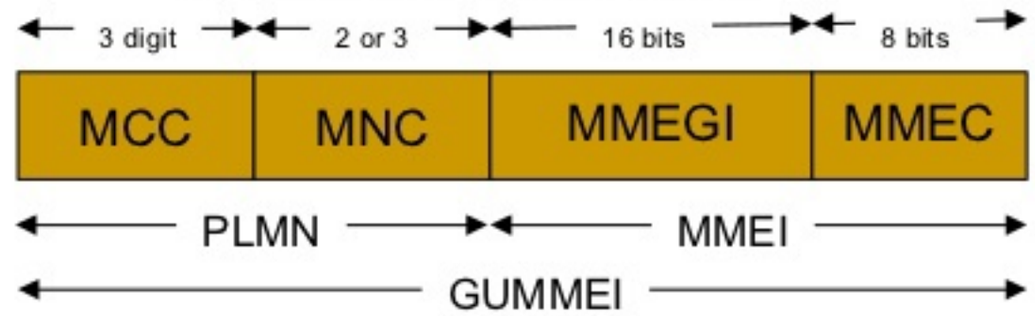
Nodes Identifiers in EPC



Tracking Area Identity (TAI)

Tracking Area Code (TAC)

Globally Unique MME Identifier

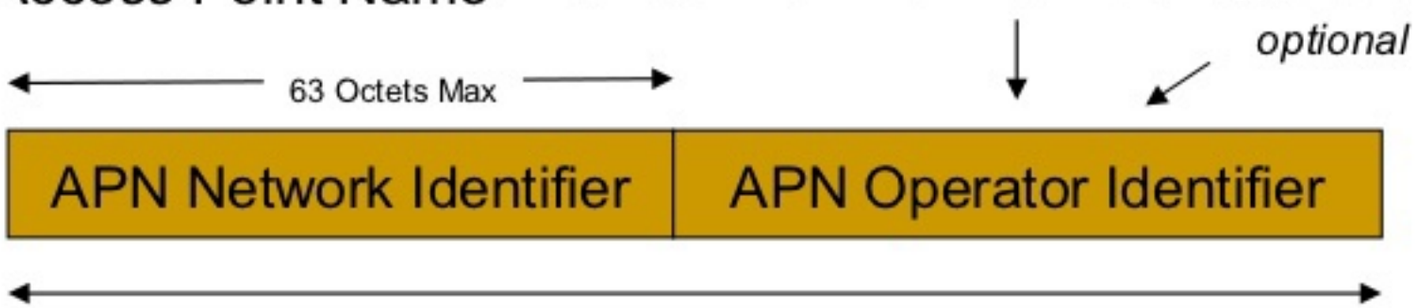


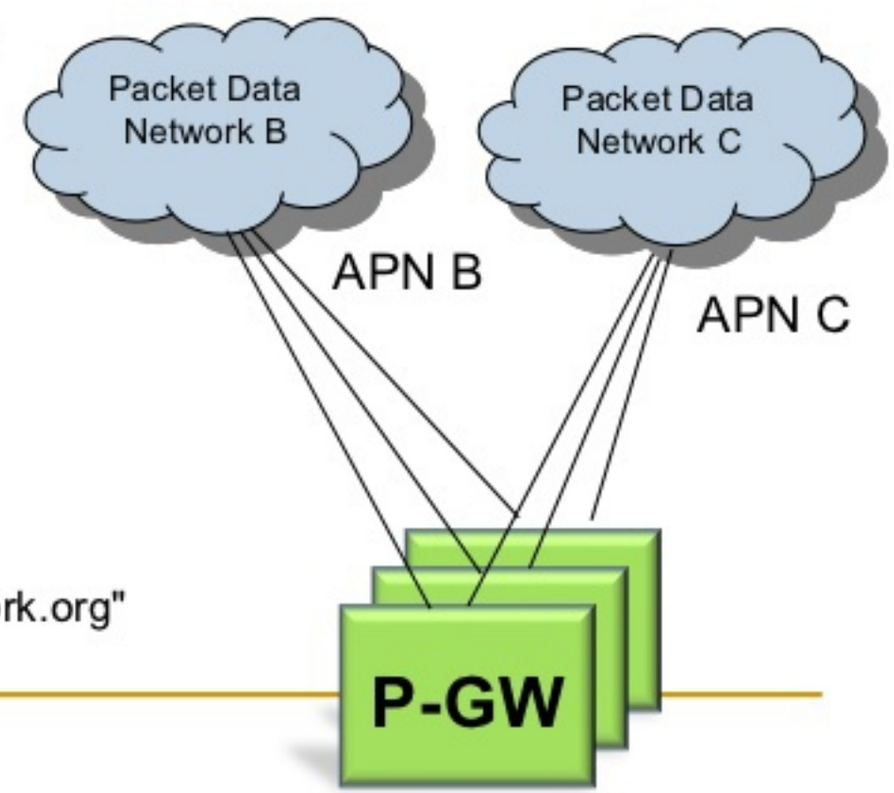
MME Identifier (MMEI)

MME Group ID (MMEGI)

MME Code (MMEC)

Access Point Name "apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

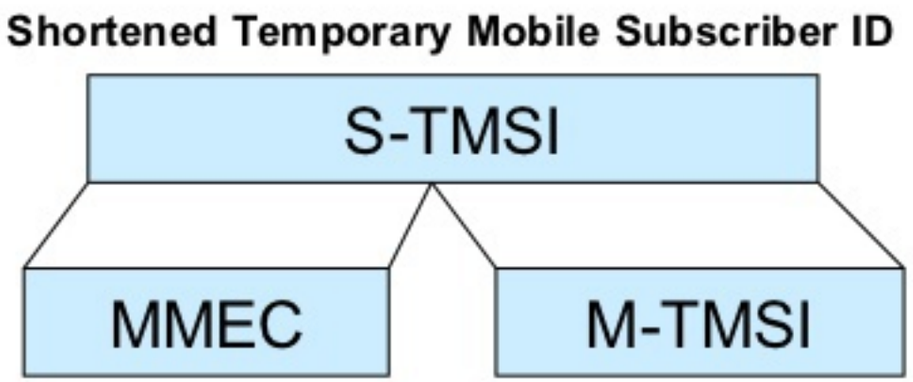


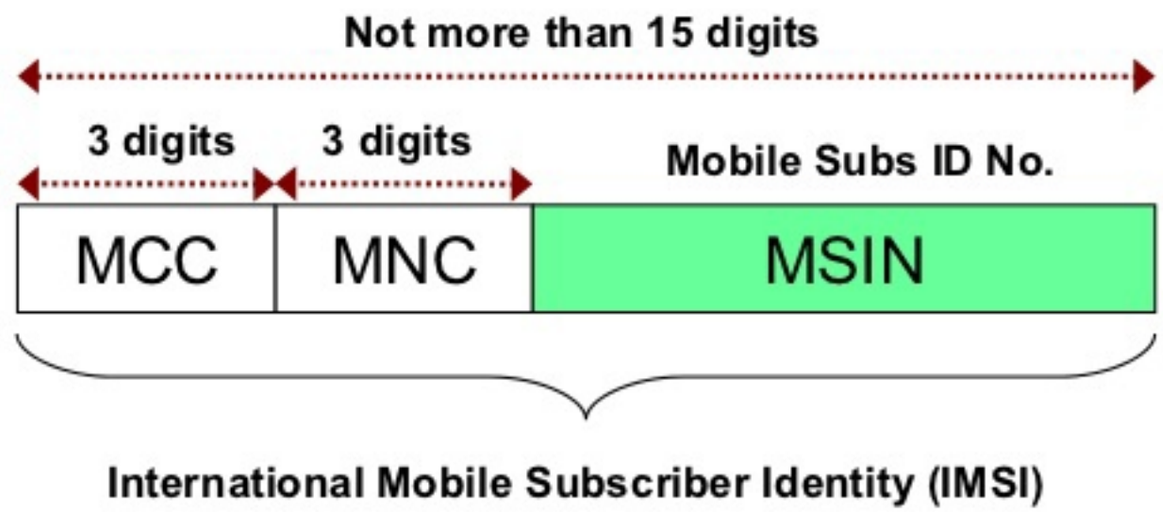


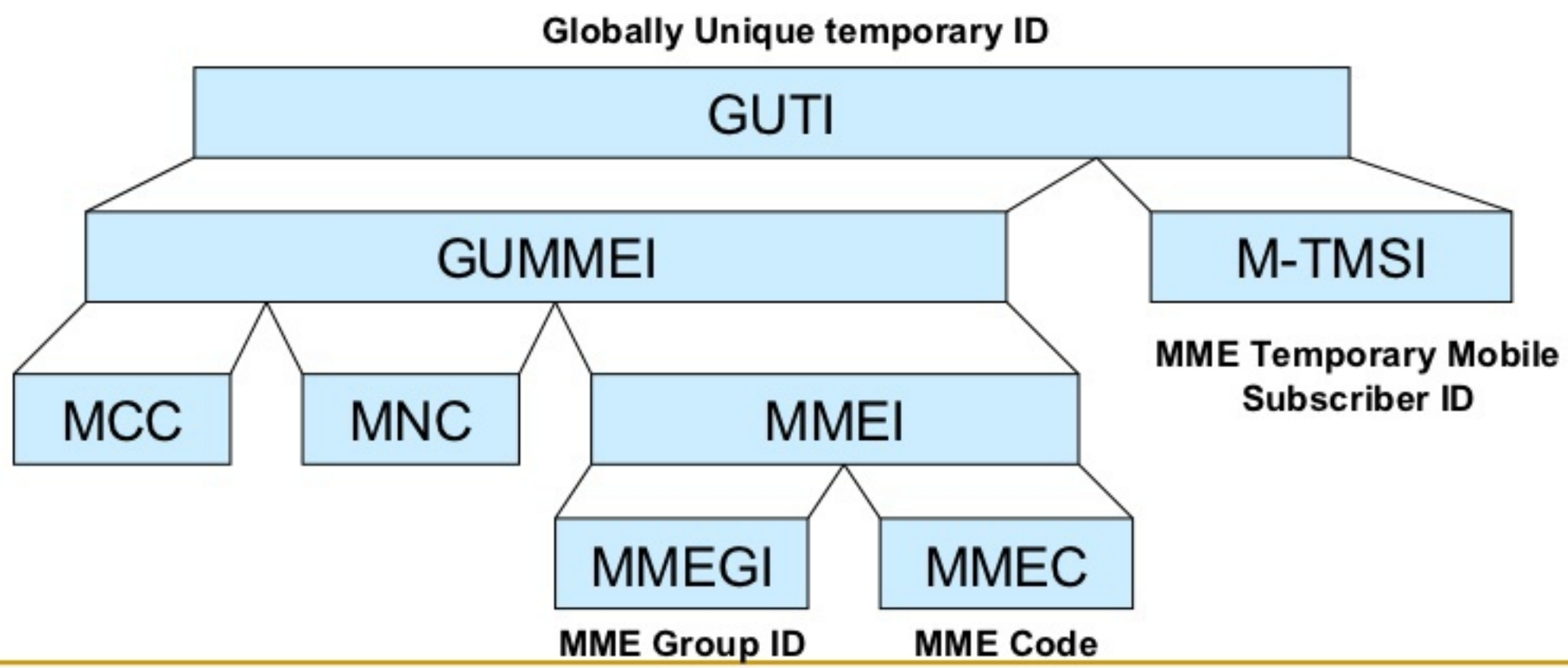
MME FQDN

“mmec<MMEC>.mmegi<MMEGI>.mme.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org"

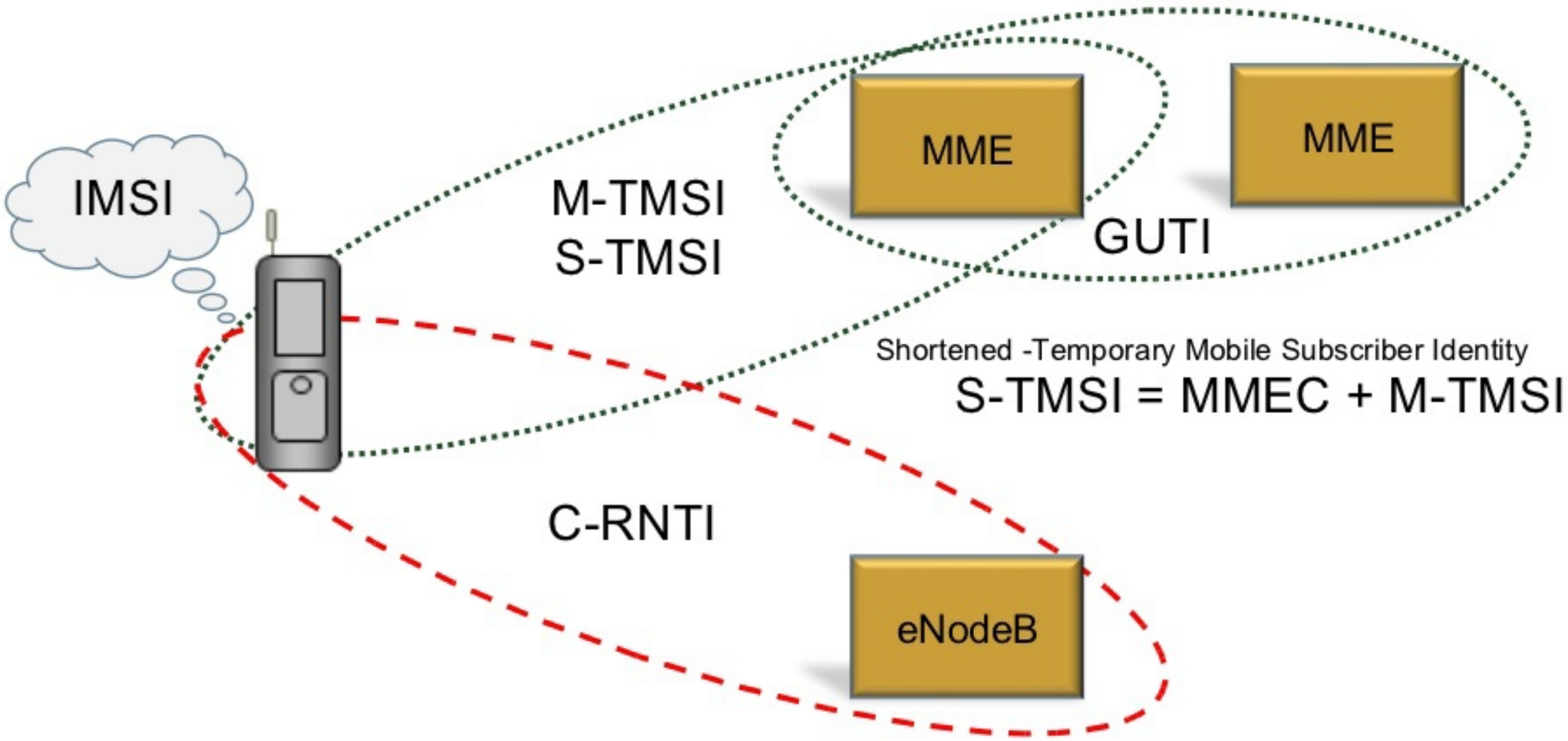
Subscriber Identifiers in EPC





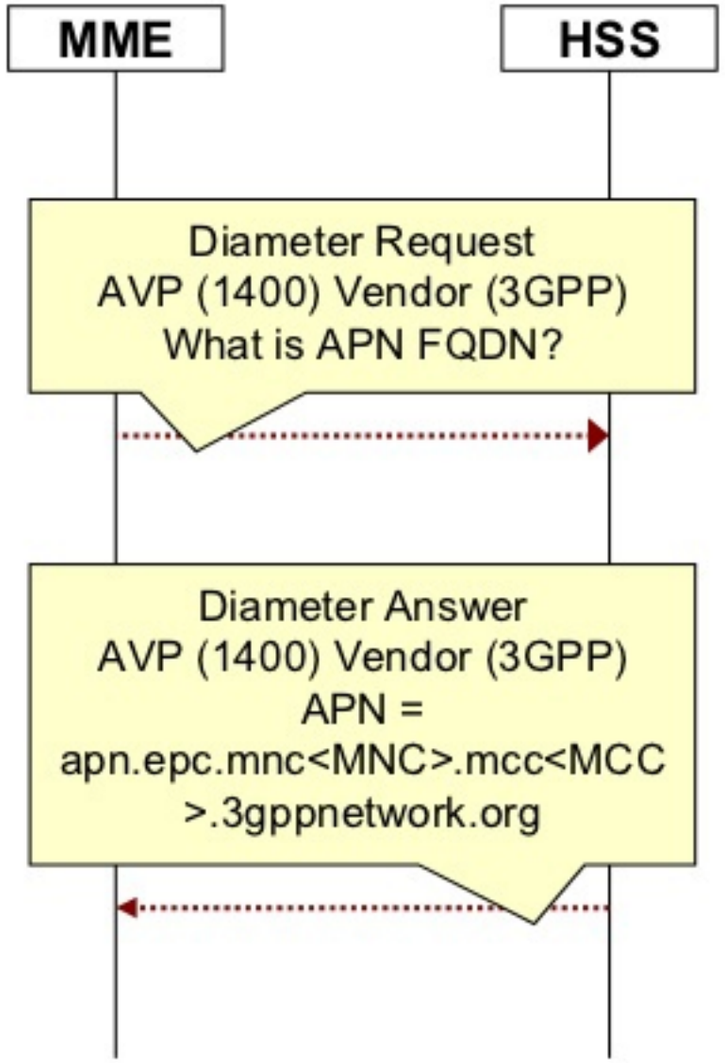


Subscriber Identifiers in EPS



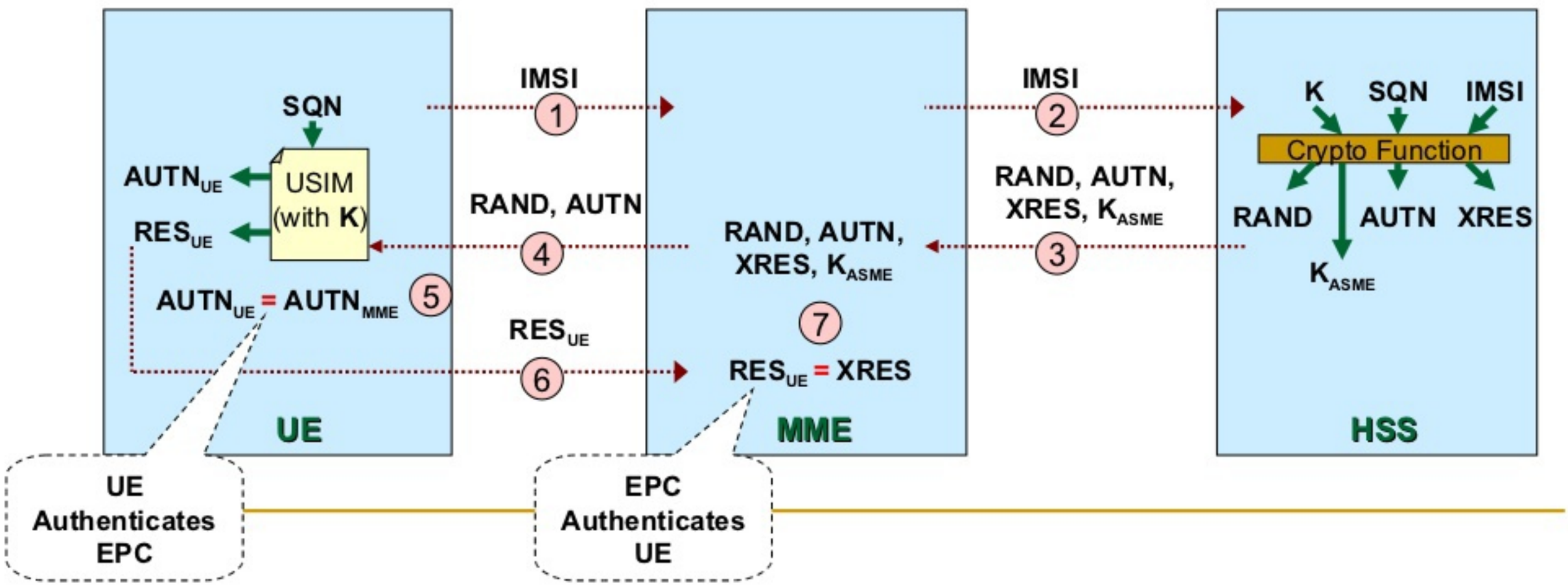
Diameter

- Diameter is the protocol of choice for HSS, PCRF, billing over S6a, Gx, Gy, Gz Interfaces.
- It conveys a collection of Attribute Value Pairs (AVP) defined in dictionary.
- Unlike Radius, it runs over TCP, 32bit AVP IDs, and provides dynamic discovery of peers.



Security

- EPC uses Authentication and Key Agreement (EPS AKA) for mutual authentication between UE and EPC.



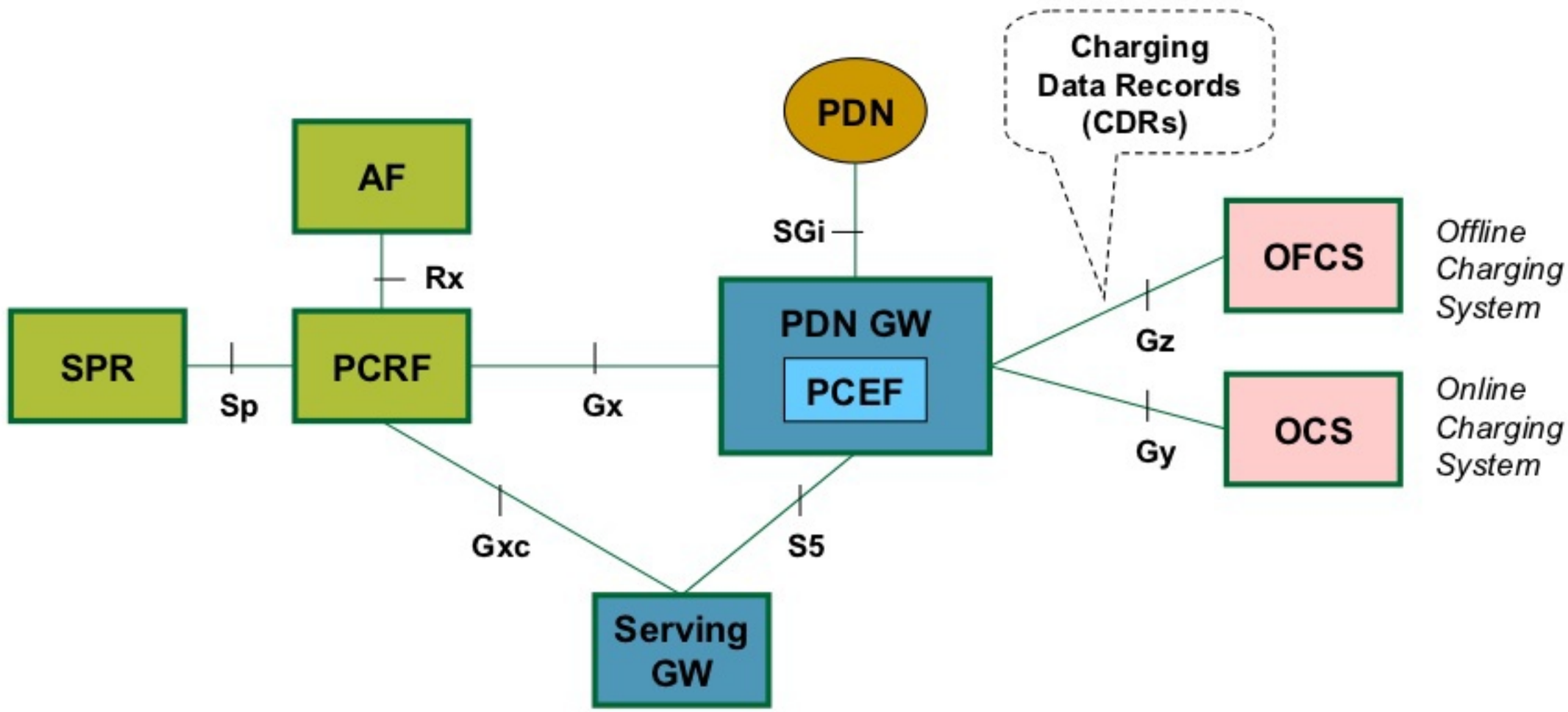
HSS User Profile

```
Subscriber {
  IMSI      = 420004000000100
  MCC       = 420
  MNC       = 004
  AUTN      = 6335A4CE3492800074B1CF6335A54E34
  RAND      = 74B0CD6031A1C8339B2B6CE2B8C4A186
  XRES      = 74B1CF6335A4CE34932266E9B4C9AF89
  KASME = 1234567890123456789012345678901234567890123456789012345678901234
  DEFAULT_QCI  = 5
  ARP_PRIORITY = 1
  APN_OI_REPLACEMENT_IND = internet
  UE_AMBR_UL = 256000000
  UE_AMBR_DL = 256000000
  APN_AMBR_UL = 256000000
  APN_AMBR_DL = 256000000
  PDNGW_IP_ADDR = 10.125.7.44
  PDNGW_NAME    = test1
}
```

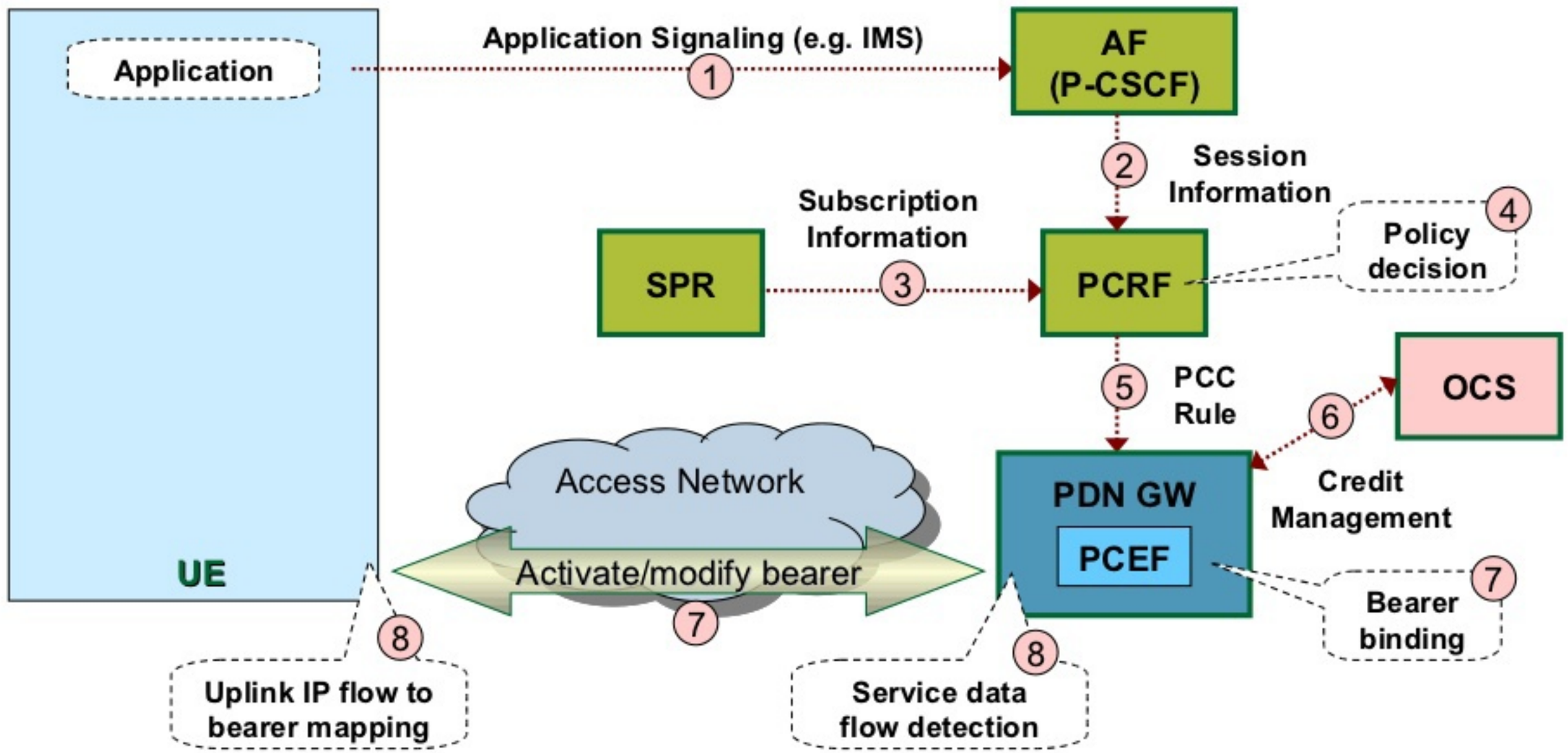
Policy and Charging Control (PCC)

- Application Function (AF): End point for Application signaling, e.g., P-CSCF in IMS. It determines what and when UE requests an application.
- Policy and Charging Rules Function (PCRF): Repository and decision point for charging and policing control.
- Policy and Charging Enforcement Function (PCEF): Resides in P-GW where rules are enforced.

Policy and Charging Control (PCC)



PCC Use Case

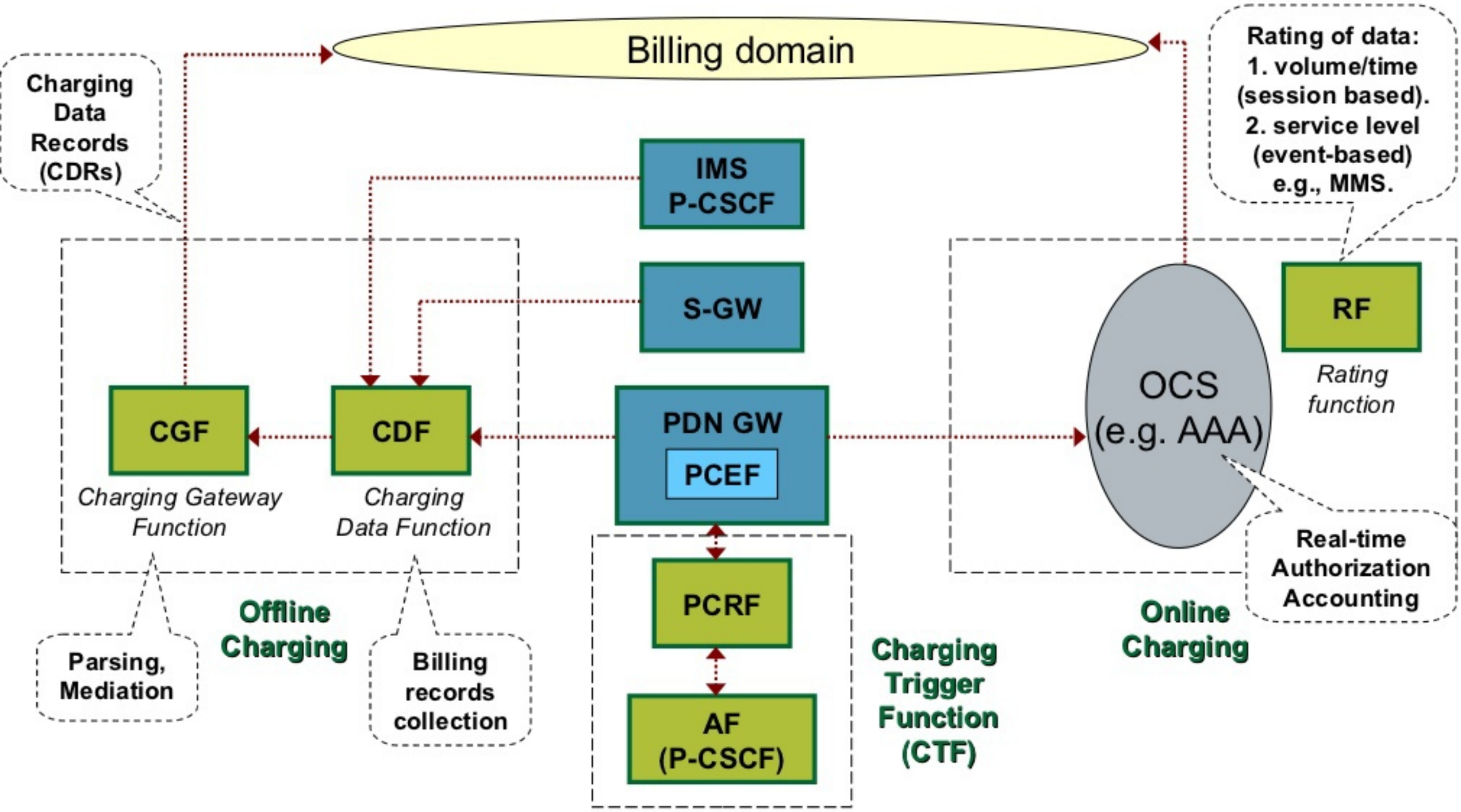

Application
Application Signaling (e.g. IMS)
1
AF
(P-CSCF)
2
Session
Information
Subscription
Information
SPR
3
PCRF
4
Policy
decision
5
PCC
Rule
6
OCS
Credit
Management
Access Network
Activate/modify bearer
7
PDN GW
PCEF
7
Bearer
binding
UE
8
Uplink IP flow to
bearer mapping
8
Service data
flow detection

Elements of PCC Rule

- Policy control functions:
  - Traffic control: e.g., block/allow IP packets.
  - QoS control: MBR, GBR, QCI, ARP.
  - Charging control: offline/online charging, data volume/duration or event-based charging.
- Subset of PCC elements from *23.203*:

Type of Element	PCC Rule Element	Comment
Rule identification	Rule identifier	Used between PCRF and PCEF for referencing PCC rules
Service Data Flow (SDF) detection information in PCEF	SDF Template Precedence	Ordered packet filters for detection of service data flow
Policy control (Gating and QoS)	Gate Status, QCI, UL/DL MBR, GBR, ARP	SDF pass or discard (gate open/closed), packet forwarding behaviour (MBR, GBR, etc.)
Charging Control	Charging key, charging method, measurement method	Tariff for SDF, charging method (online, offline, volume, duration, event-driven)

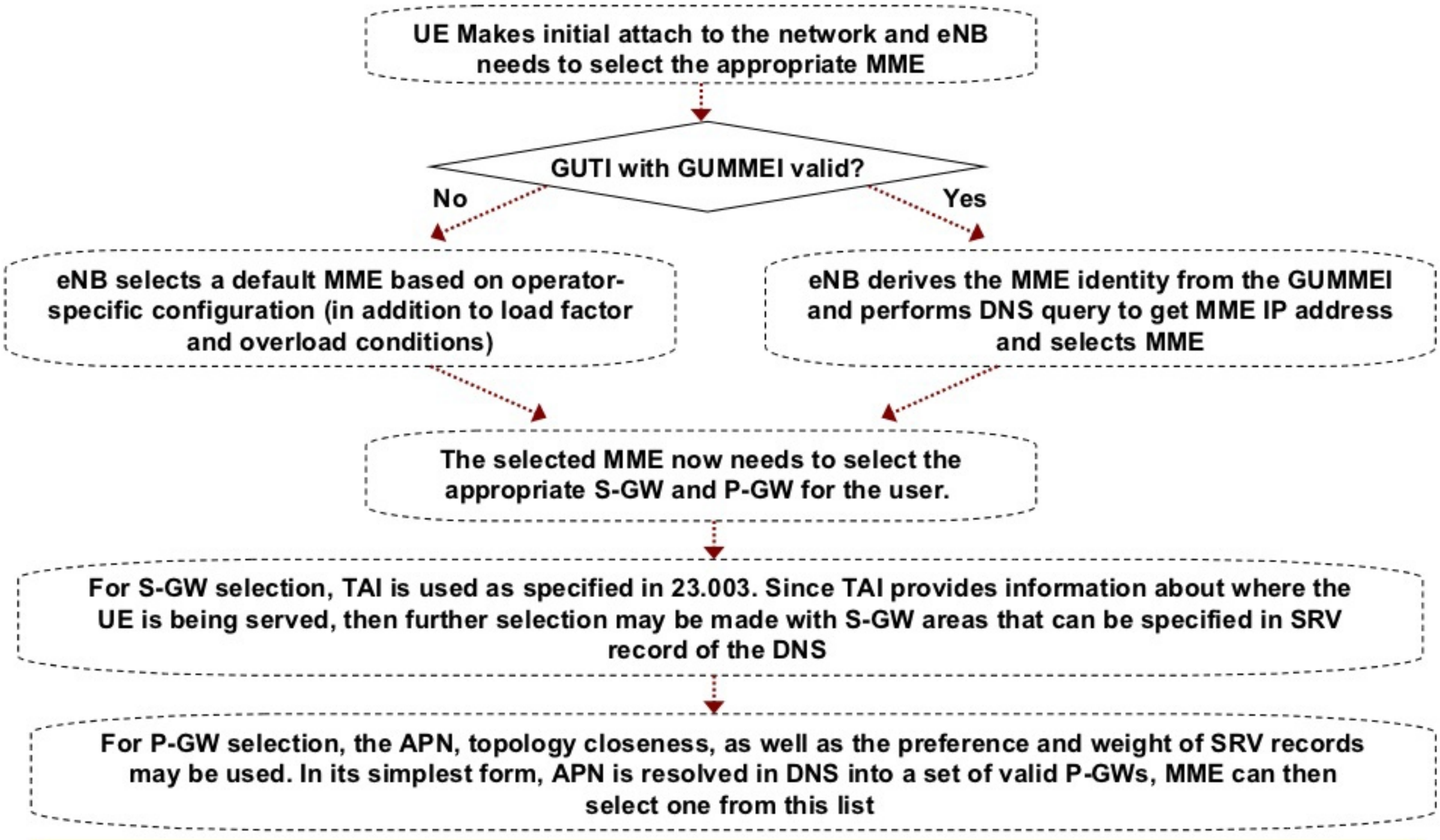
Charging


Billing domain
Charging Data Records (CDRs)
Rating of data:
1. volume/time (session based).
2. service level (event-based) e.g., MMS.
IMS P-CSCF
S-GW
RF
Rating function
OCS (e.g. AAA)
CGF
CDF
PDN GW
PCEF
Charging Gateway Function
Charging Data Function
Real-time Authorization Accounting
PCRF
Offline Charging
Online Charging
Parsing, Mediation
Billing records collection
Charging Trigger Function (CTF)
AF (P-CSCF)

Charging Data Records (CDRs) Contents

Field	Example	Comments
Served IMSI	418300400796343	IMSI of the served party
Served IMEI	3532460164156301	IMEI of the served party
Charging ID	3292529918	Billing record identifier
PGW Address	10.34.5.67	Serving P-GW IP address
APN ID	internet.epc.mnc3.mcc418.3gppnetwork.org	FQDN of the connected APN
Duration	180 sec	Duration of this record
Uplink Volume	5629 bytes	Amount of UL data
Downlink Volume	20678 bytes	Amount of DL data
Tracking Area Code	15	TAC ID
Cause for Record Closing	Normal Release	The reason for release of record

Selection Function



Further Readings

- 3GPP Technical Specification 23.002, “SAE Network Architecture” (Release 8) www.3gpp.org.
- 3GPP Technical Specification 23.203, “PCC Architecture” (Release 8) www.3gpp.org.
- 3GPP Technical Specification 33.401, “SAE: Security Architecture (Release 8) www.3gpp.org.
- 3GPP Technical Specification 29.272, “EPS; MME and SGSN related interfaces based on Diameter protocol” (Release 8) www.3gpp.org.