EURECOM

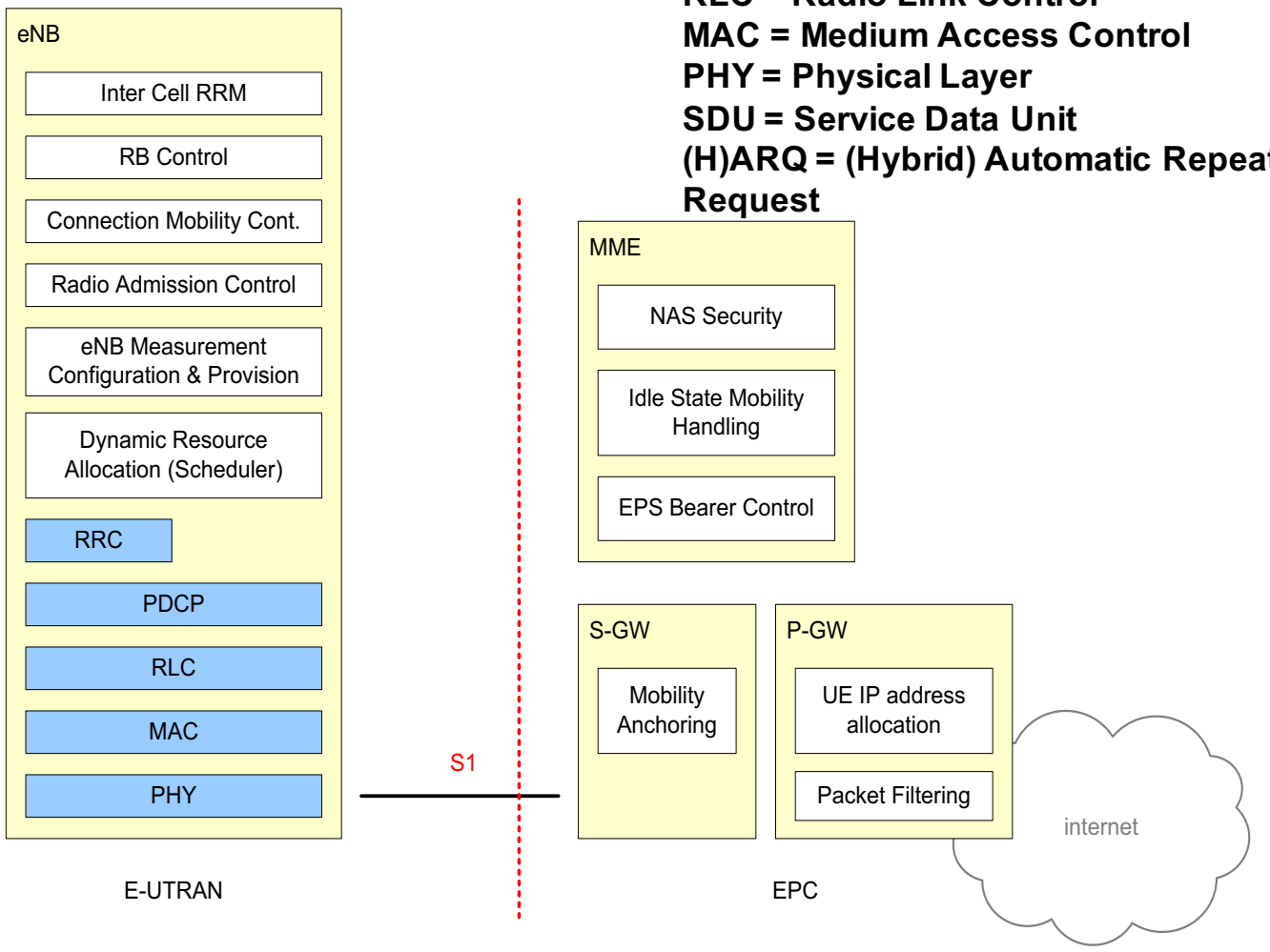
Sophia Antipolis

Evolved Packet Core (EPC)

Adlen Ksentini

EPC Functions

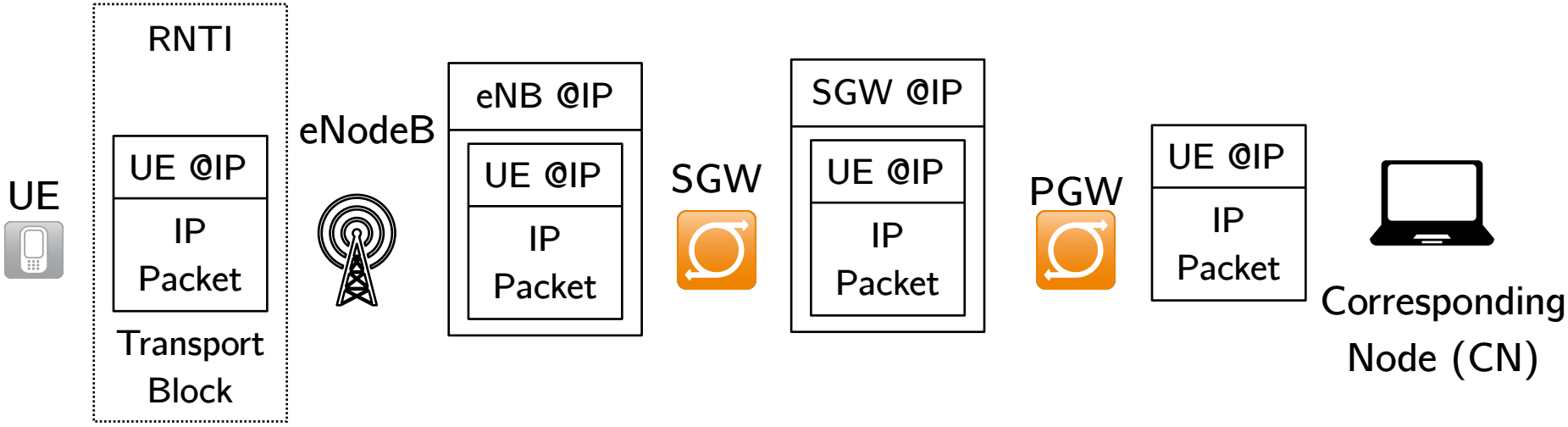
PDCP = Packet Data Convergence Protocol
RLC = Radio Link Control
MAC = Medium Access Control
PHY = Physical Layer
SDU = Service Data Unit
(H)ARQ = (Hybrid) Automatic Repeat Request



Data plane management

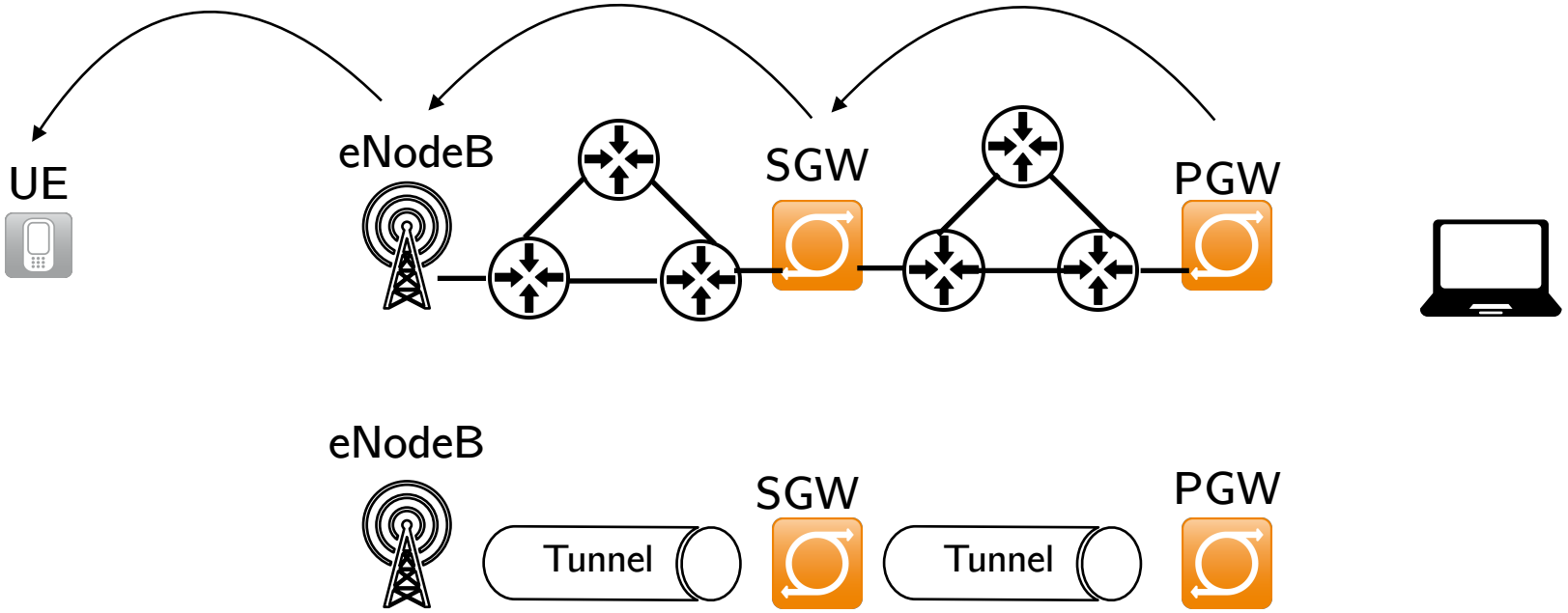
Concept of packet encapsulation

- Same IP prefix is used by all the mobile network subscriber
  - IP prefix changes with mobility in the Internet
- Encapsulation consists in encapsulating one IP packet inside another IP packet



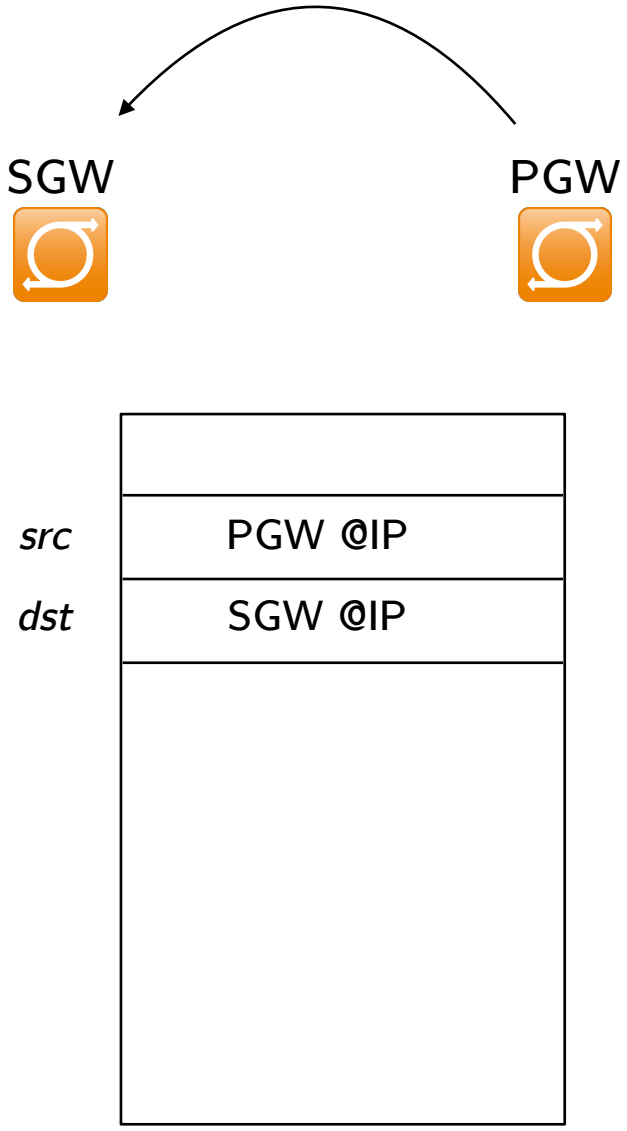
Tunneling concept

- Whatever the network topology, a packet always goes from the PGW to the SGW, like having a tunnel between the PGW and SGW

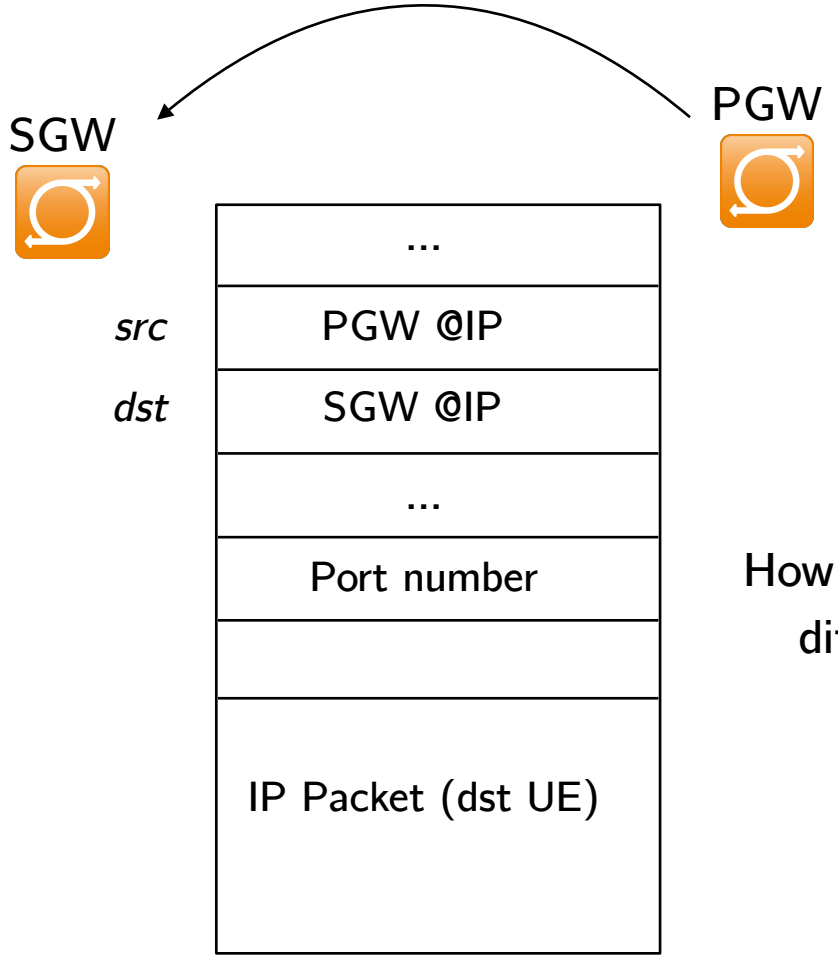


Layer 4 protocol

- The PGW always sends received packets to the SGW
  - It is not aware about what happen after the SGW
- A need for a transport protocol
  - TCP: too complex
  - UDP: simple. The reliability needs to be handled by the higher layers
- UDP
  - Between SGW and PGW
  - Between eNodeB and PGW



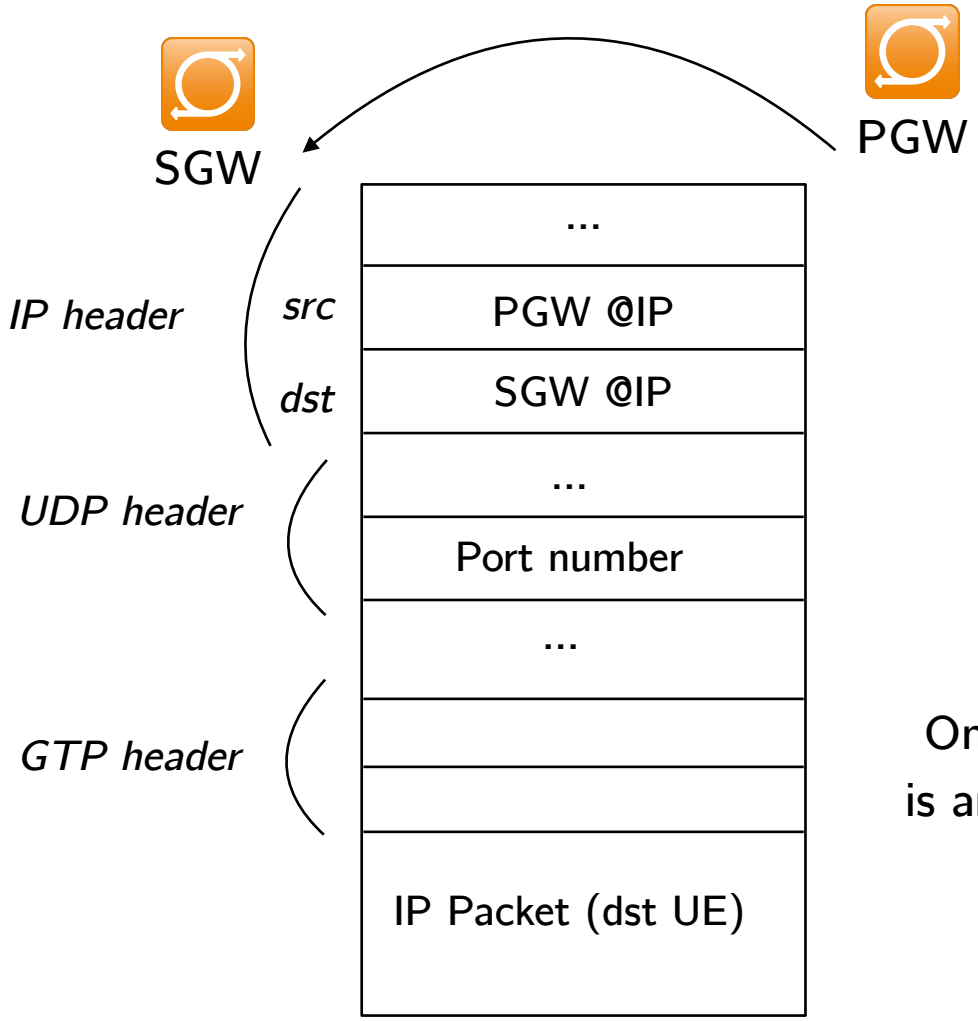
New layer



IPv4? IPv6?
How to avoid handling different format?

- An additional layer (new protocol, new format)
  - GTP, GPRS Tunneling protocol

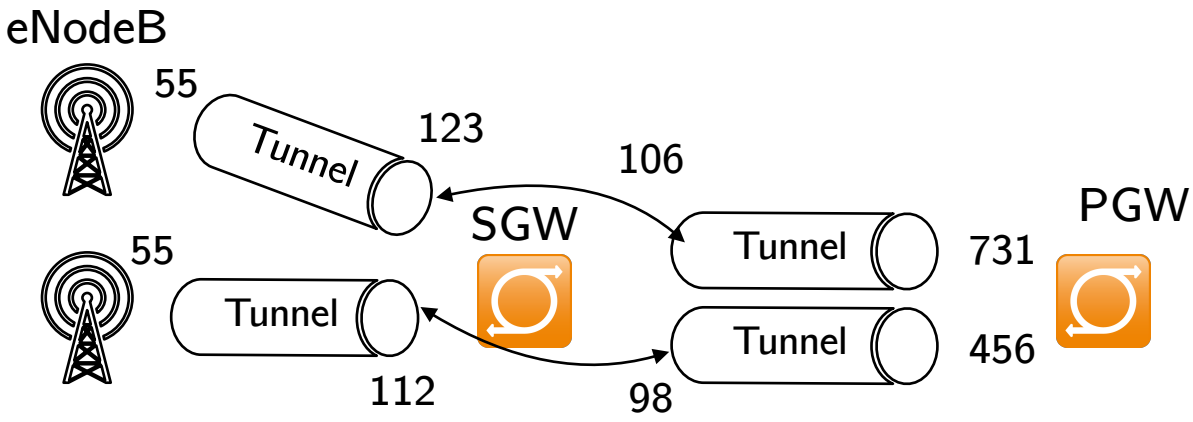
GTP-U



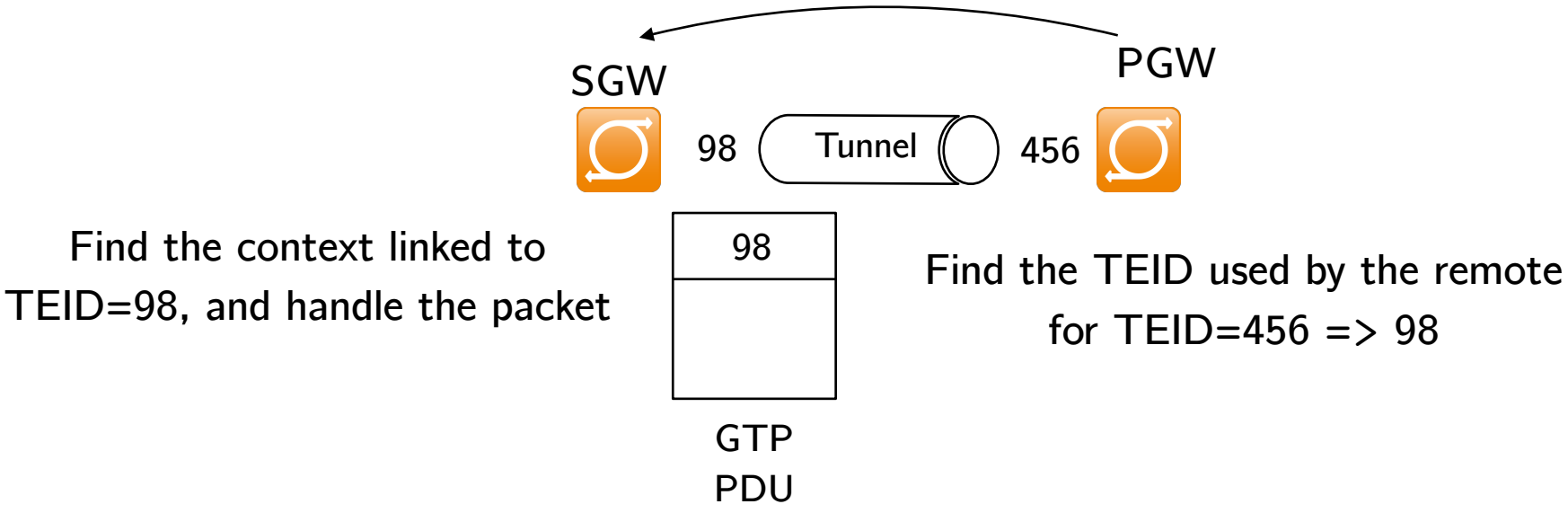
Only the GTP header
is analyzed by the xGW

GTP-U

- GTP-U runs on top of UDP
  - Simplicity by report to TCP. For reliability, it is end-to-end
  - Tunnel End points Identifier (TEID) 32 bits to identify the end point of a tunnel
  - Each tunnel is identified by a pair of TEID
  - Exchanged via the GTP-C



GTP-U forwarding process

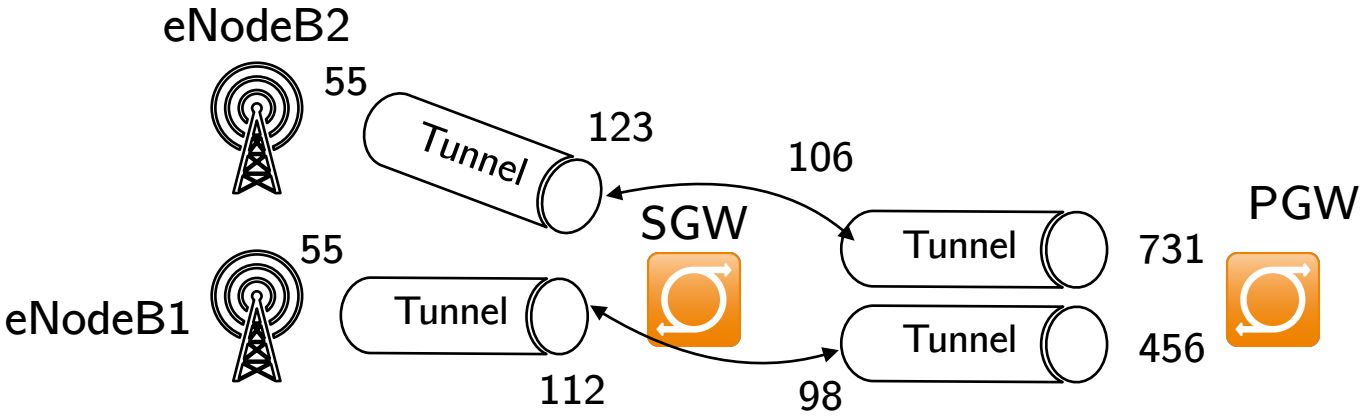


- The sender should know the TEID used by the remote
- Very simple receiver

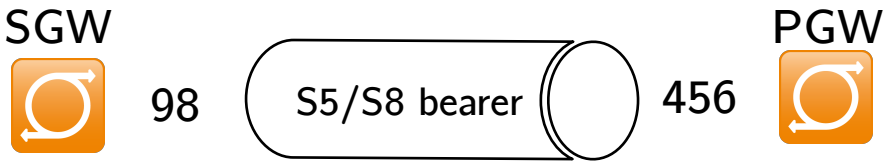
GTP-U TEID management

SGW Table

TEID	Action	Details	Peer entity	
			IP@	TEID
98	Forward	TEID=112	PGW IP@	456
106	Forward	TEID=123	PGW IP@	731
112	Forward	TEID=98	eNodeB1 IP@	55
123	Forward	TEID=106	eNodeB2 IP@	55



Tunnel set-up



Select a new value locally unique TEID 98

Set-up a tunnel with TEID=98

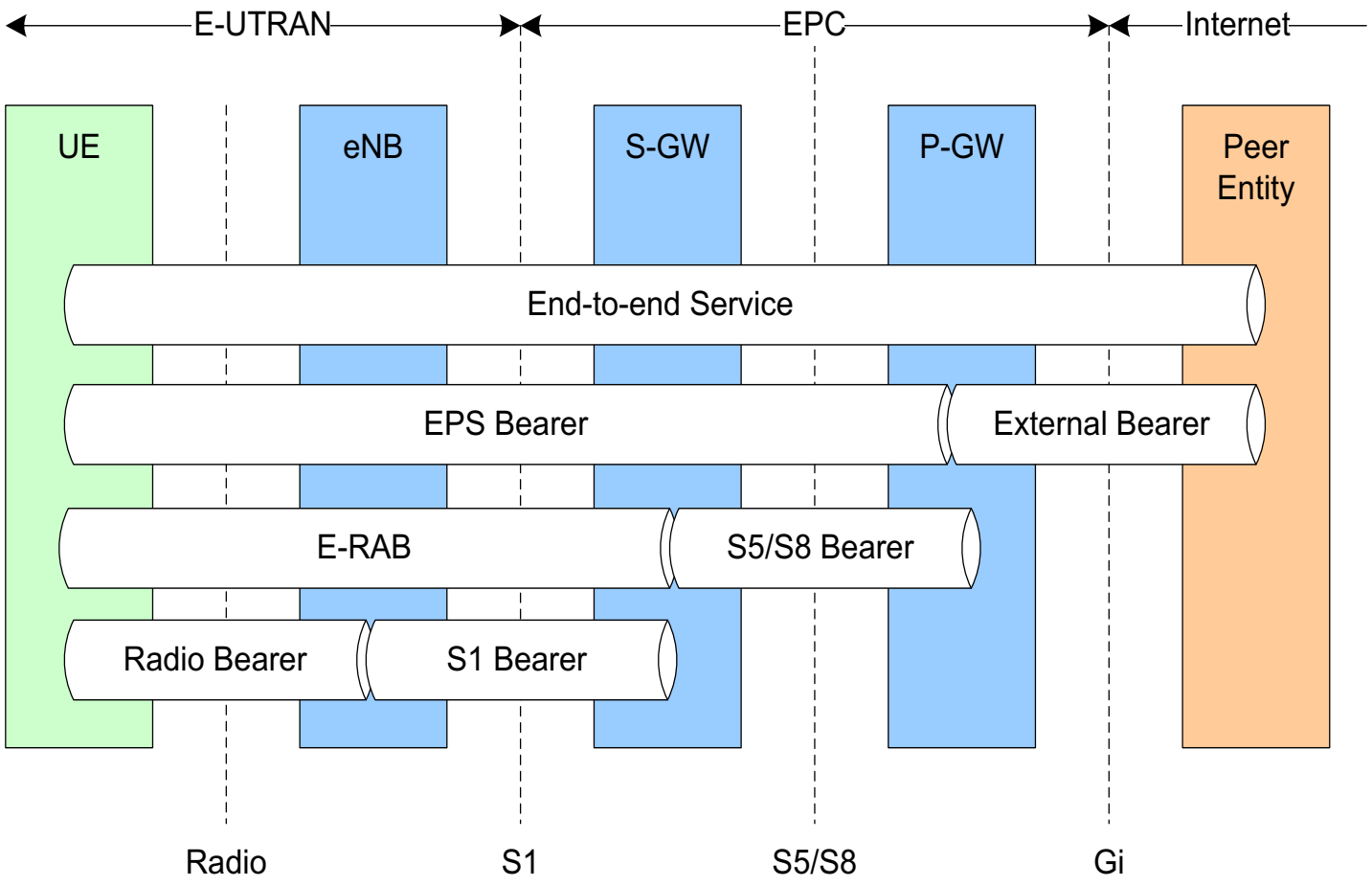
1. Select a new value (locally unique) 456
2. Save the @IP of the remote
3. Save the received TEID and links it with 456-SGW@/98

ACK TEID=456, TEID=98

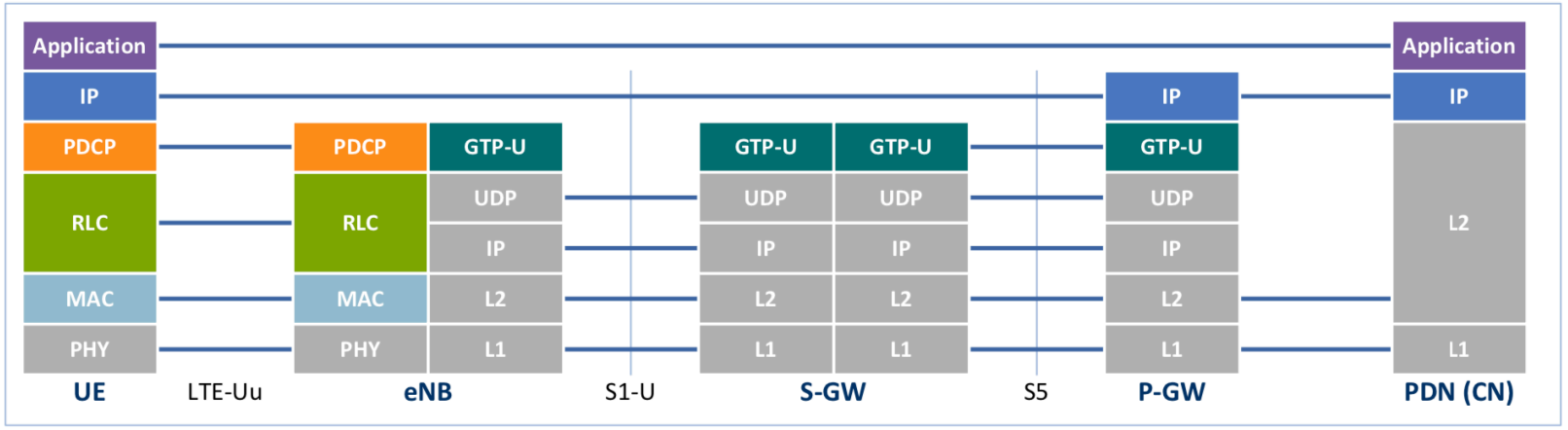
1. Save the @IP of the remote
2. Save the received TEID and links it with 98-PGW@/456

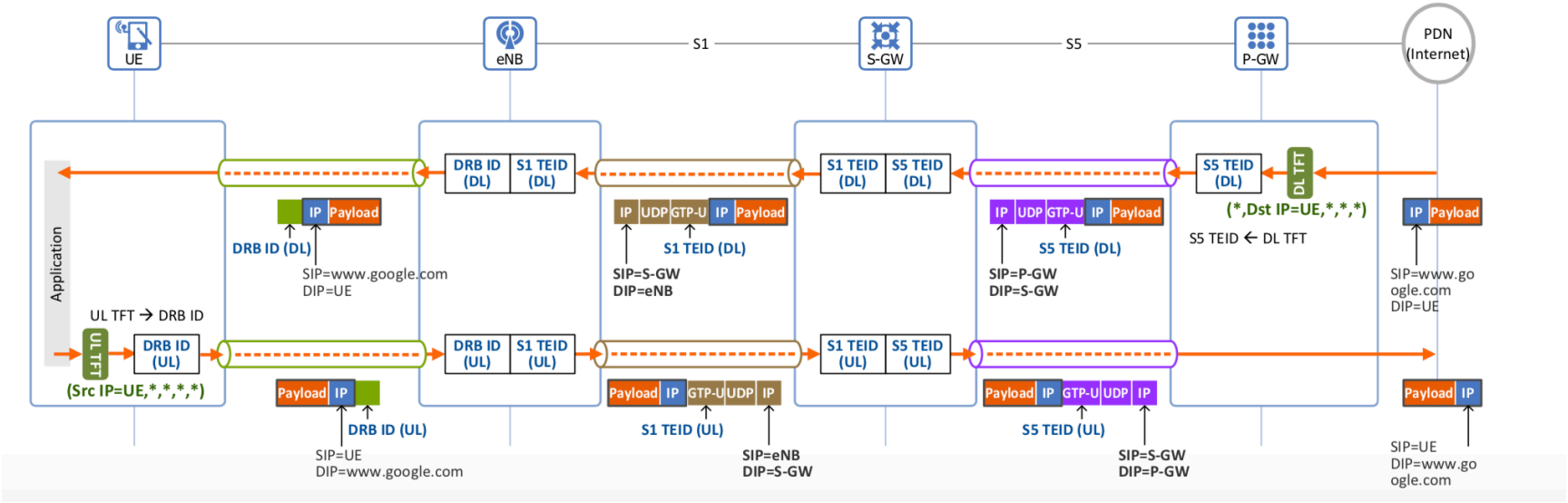
- GTP-C protocol used to establish and manage GTP-U tunnel

LTE Bearers


E-UTRAN
EPC
Internet
UE
eNB
S-GW
P-GW
Peer Entity
End-to-end Service
EPS Bearer
External Bearer
E-RAB
S5/S8 Bearer
Radio Bearer
S1 Bearer
Radio
S1
S5/S8
Gi

Default Bearer structure





QoS and LTE bearer structure

- Quality of service
  - GBR bearer: Guaranteed bit rate
  - Non-GBR bearer No guaranteed bit rate
  - Default bearer Established when UE connects to PDN
  - Provides always-on connectivity
  - Always non-GBR
- Dedicated bearer Established later
  - Can be GBR or non-GBR
- Every EPS bearer
  - QoS class identifier (QCI) (error rate and delay associated with service)
  - Allocation and Retention priority (ARP) (bearer may be dropped in case of emergency)
- Every GBR bearer
  - Guaranteed bit rate (GBR) (long term average bit rate a user can expect to receive)
  - Maximum bit rate (MBR) (max instantaneous bit rate the NW may offer)
- Non-GBR bearers, collectively
  - Per APN (Access Point Name) aggregate maximum bit rate (APN-AMBR)
  - Per UE aggregate maximum bit rate (UE-AMBR)

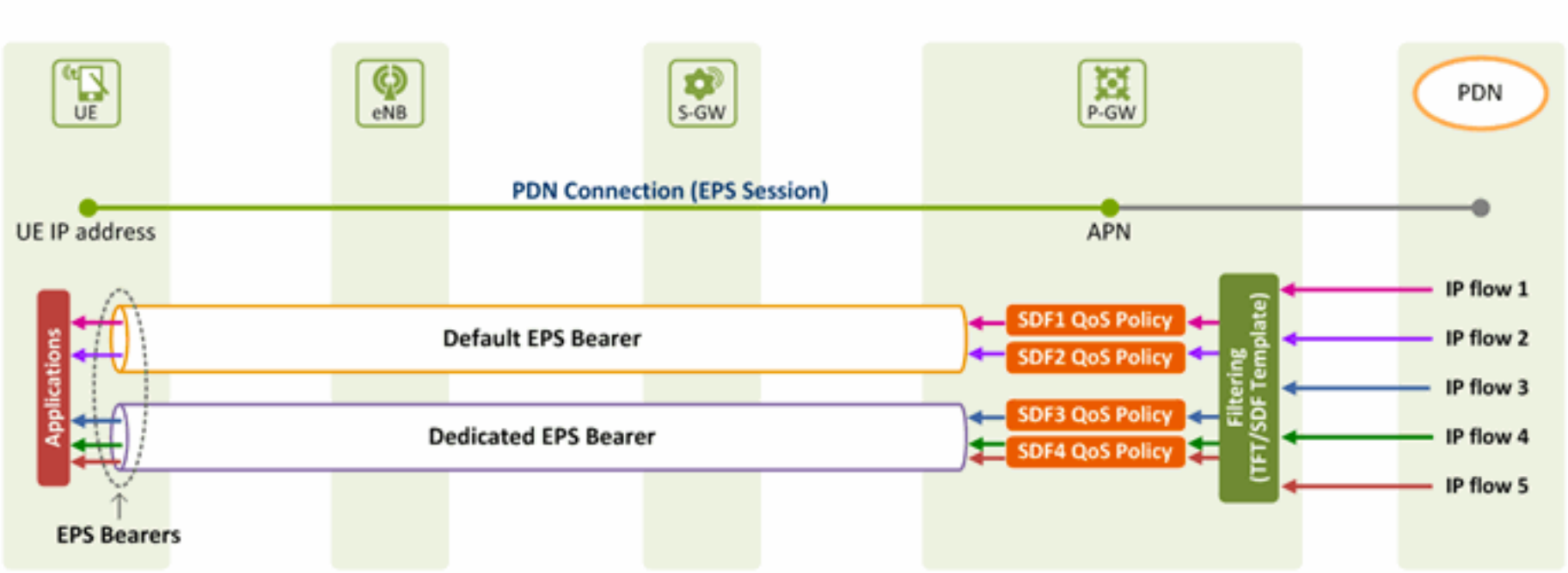
LTE QoS

QCI	Bearer Type	Application Example	Packet Delay	Packet Loss	Priority
1	GBR	Conversational VoIP	100ms	10^{-2}	2
2		Conversational Video (Live Streaming)	150ms	10^{-3}	4
3		Non-Conversational Video (Buffered Streaming)	300ms	10^{-6}	5
4		Real Time Gaming	50ms	10^{-3}	3
5	NON-GBR	IMS Signaling	100ms	10^{-6}	1
6		Voice, Video, Interactive Games	100ms	10^{-3}	7
7		Video (Buffered Streaming)	300ms	10^{-6}	6
8		TCP apps (web, email, ftp)			8
9		Platinum vs. gold user			9

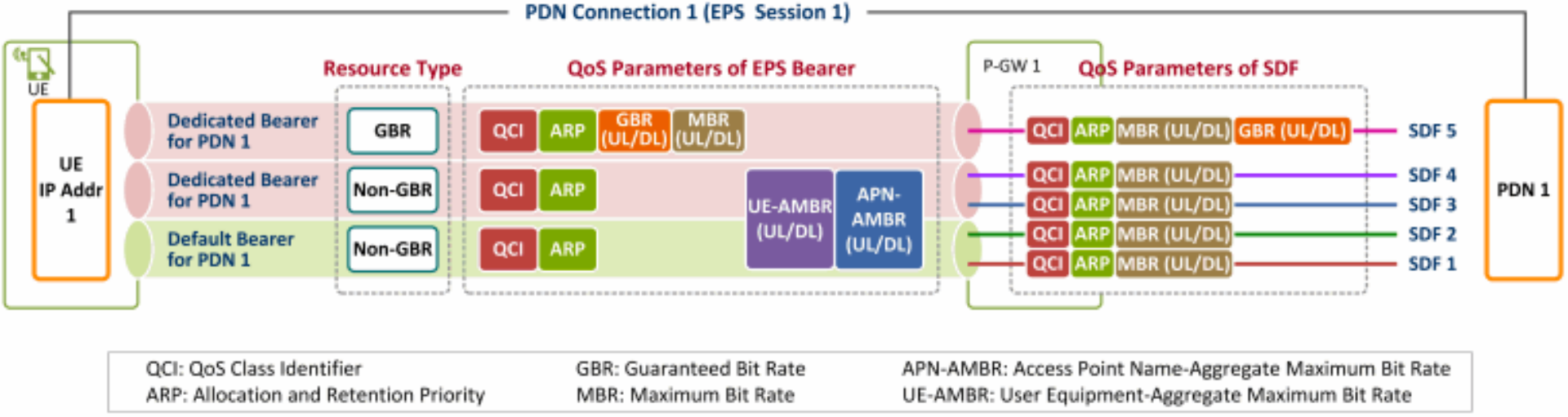
LTE QoS

- Service Data Flow (SDF)
  - An IP flow or an aggregate of IP flows of user traffic classified by the service type, using SDF template or Traffic Flow Template (TFT) (or ACL in classical routers)
  - Different QoS is applied to each SDF, each SDF is subject to different QoS rules determined by PCRF
  - Each SDF is delivered through an EPS bearer that can satisfy its QoS
  - A SDF that matches the packet filters of a TFT is mapped to an EPS bearer, and multiple SDFs with the same QCI are mapped and delivered to one EPS bearer
  - Each EPS bearer is activated with QoS parameters that indicate the characteristics of the transmission path

LTE QoS


UE
eNB
S-GW
P-GW
PDN
PDN Connection (EPS Session)
UE IP address
APN
Applications
Default EPS Bearer
Dedicated EPS Bearer
EPS Bearers
SDF1 QoS Policy
SDF2 QoS Policy
SDF3 QoS Policy
SDF4 QoS Policy
Filtering (TFT/SDF Template)
IP flow 1
IP flow 2
IP flow 3
IP flow 4
IP flow 5

LTE QoS



QCI: QoS Class Identifier	GBR: Guaranteed Bit Rate	APN-AMBR: Access Point Name-Aggregate Maximum Bit Rate
ARP: Allocation and Retention Priority	MBR: Maximum Bit Rate	UE-AMBR: User Equipment-Aggregate Maximum Bit Rate

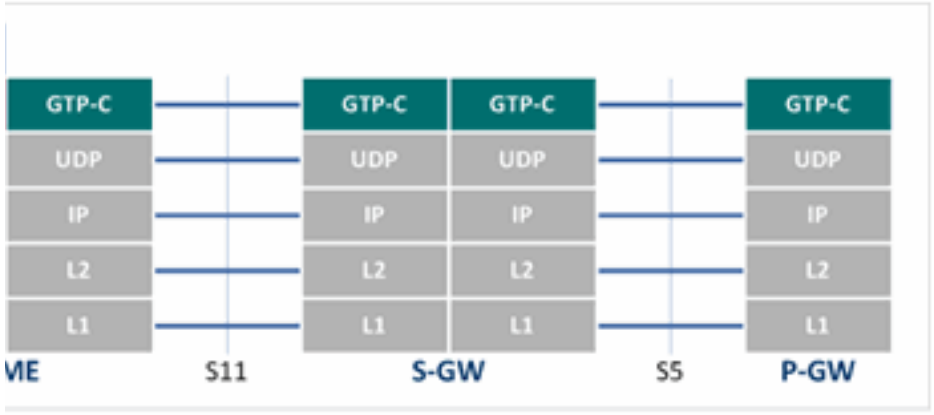
LTE QoS

```
29 5.980770335   fd00:0:0:3::100      fd00:0:0:4::191      GTPv2     197 Create Bearer Request

▼ EPS Bearer Level Traffic Flow Template (Bearer TFT) :
    IE Type: EPS Bearer Level Traffic Flow Template (Bearer TFT) (84)
    IE Length: 19
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    001. .... = TFT operation code: Create new TFT (1)
    ...0 .... = E bit: Parameters list is not included
    .... 0001 = Number of packet filters: 1
  ▼ Packet filter: 0
      00.. .... = Spare bit(s): 0
      ..11 .... = Packet filter direction: Bidirectional (3)
      .... 0000 = Packet filter identifier: 1 (0)
      Packet evaluation precedence: 0xfd (253)
      Packet filter length: 0x0f (15)
    ▼ Packet filter component type identifier: Single remote port type (80)
        Port: 2020
    ▼ Packet filter component type identifier: IPv4 remote address type (16)
        IPv4 address: 1.2.2.4
        IPv4 address mask: 255.255.255.255
    ▼ Packet filter component type identifier: Single local port type (64)
        Port: 1010
▼ Bearer Level Quality of Service (Bearer QoS) :
    IE Type: Bearer Level Quality of Service (Bearer QoS) (80)
    IE Length: 22
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    .1.. .... = PCI (Pre-emption Capability): Disabled
    ..11 00.. = PL (Priority Level): 12
    .... ...1 = PVI (Pre-emption Vulnerability): Disabled
    Label (QCI): 5
```

LTE QoS

```
29 5.980770335   fd00:0:0:3::100      fd00:0:0:4::191      GTPv2     197 Create Bearer Request

▼ EPS Bearer Level Traffic Flow Template (Bearer TFT) :
    IE Type: EPS Bearer Level Traffic Flow Template (Bearer TFT) (84)
    IE Length: 19
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    001. .... = TFT operation code: Create new TFT (1)
    ...0 .... = E bit: Parameters list is not included
    .... 0001 = Number of packet filters: 1
  ▼ Packet filter: 0
      00.. .... = Spare bit(s): 0
      ..11 .... = Packet filter direction: Bidirectional (3)
      .... 0000 = Packet filter identifier: 1 (0)
      Packet evaluation precedence: 0xfd (253)
      Packet filter length: 0x0f (15)
    ▼ Packet filter component type identifier: Single remote port type (80)
        Port: 2020
    ▼ Packet filter component type identifier: IPv4 remote address type (16)
        IPv4 address: 1.2.2.4
        IPv4 address mask: 255.255.255.255
    ▼ Packet filter component type identifier: Single local port type (64)
        Port: 1010
▼ Bearer Level Quality of Service (Bearer QoS) :
    IE Type: Bearer Level Quality of Service (Bearer QoS) (80)
    IE Length: 22
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    .1.. .... = PCI (Pre-emption Capability): Disabled
    ..11 00.. = PL (Priority Level): 12
    .... ...1 = PVI (Pre-emption Vulnerability): Disabled
    Label (QCI): 5
```

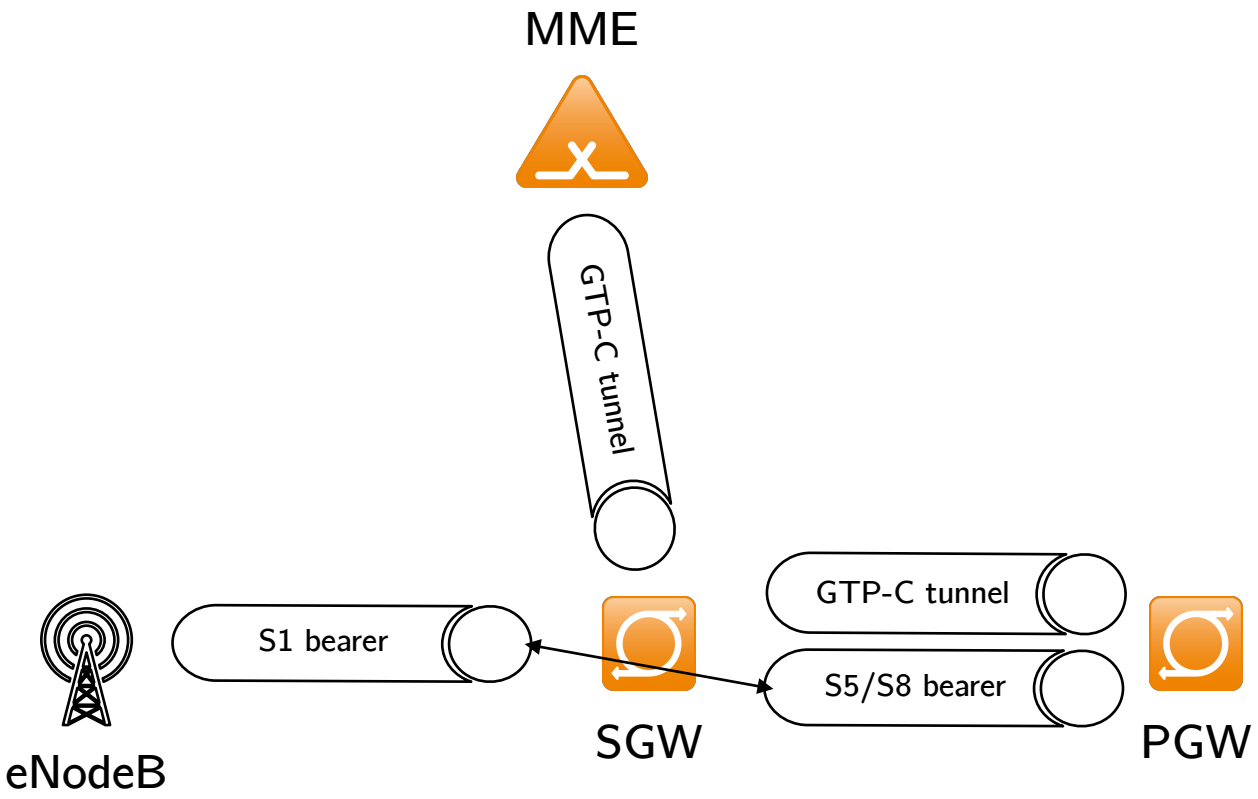
GTP-C



- Used to control messages to control GTP tunnels (ex. generation and instantiating of TEID)
  - Usually come in Request/Response pairs
  - Create/Delete Session Request/Response
  - Create/Delete Bearer Request/Response
  - Modify Bearer Request/Response

GTP-C

Each Tunnel is identified by a TEID pair



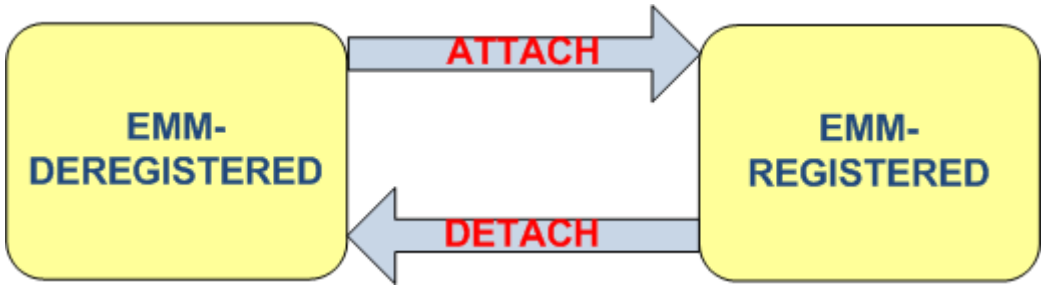
LTE Mobility Management

EMM: EPS Mobility Management

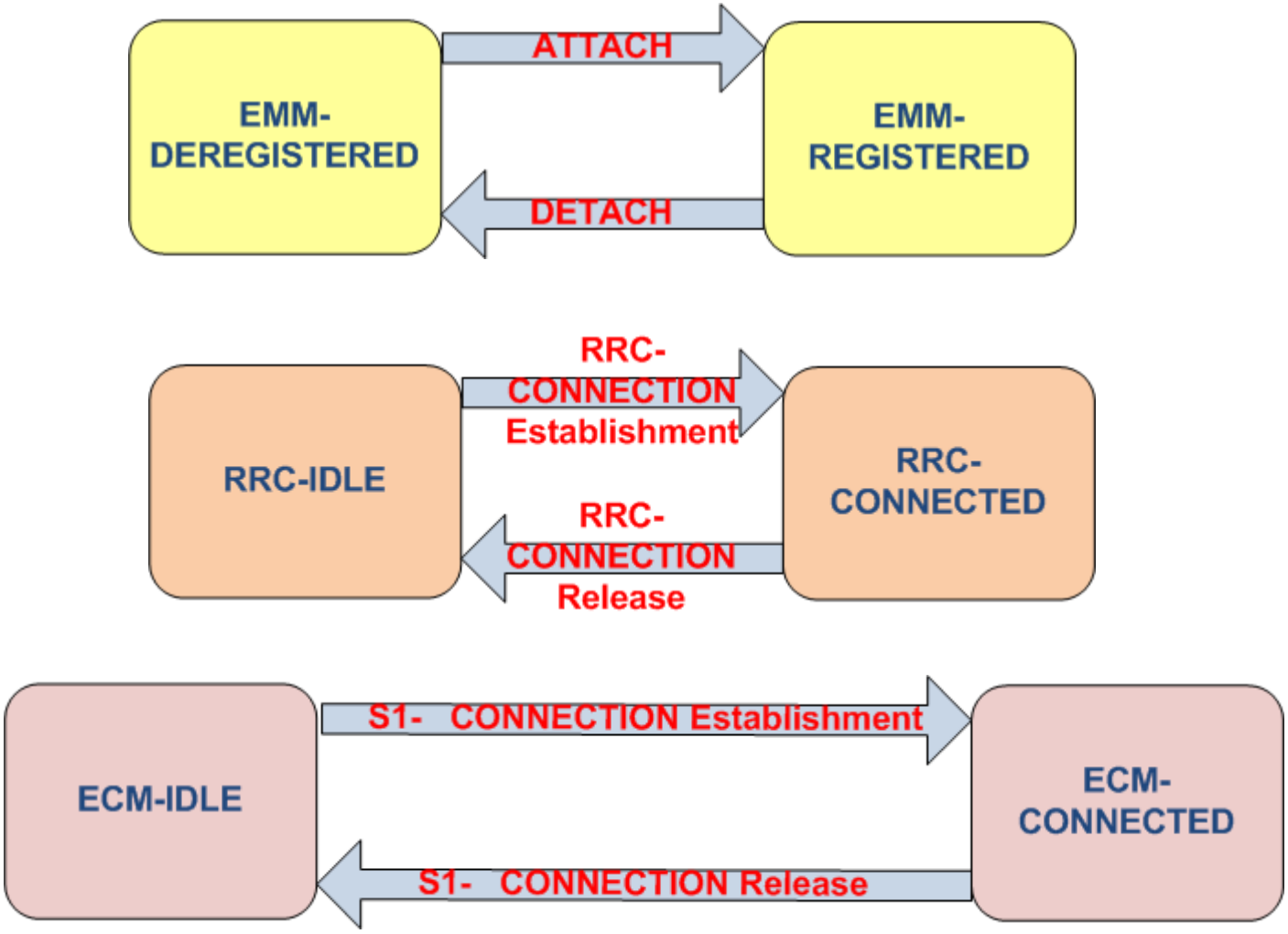
ECM: EPS Connection Management

General procedures: LTE Mobility Management

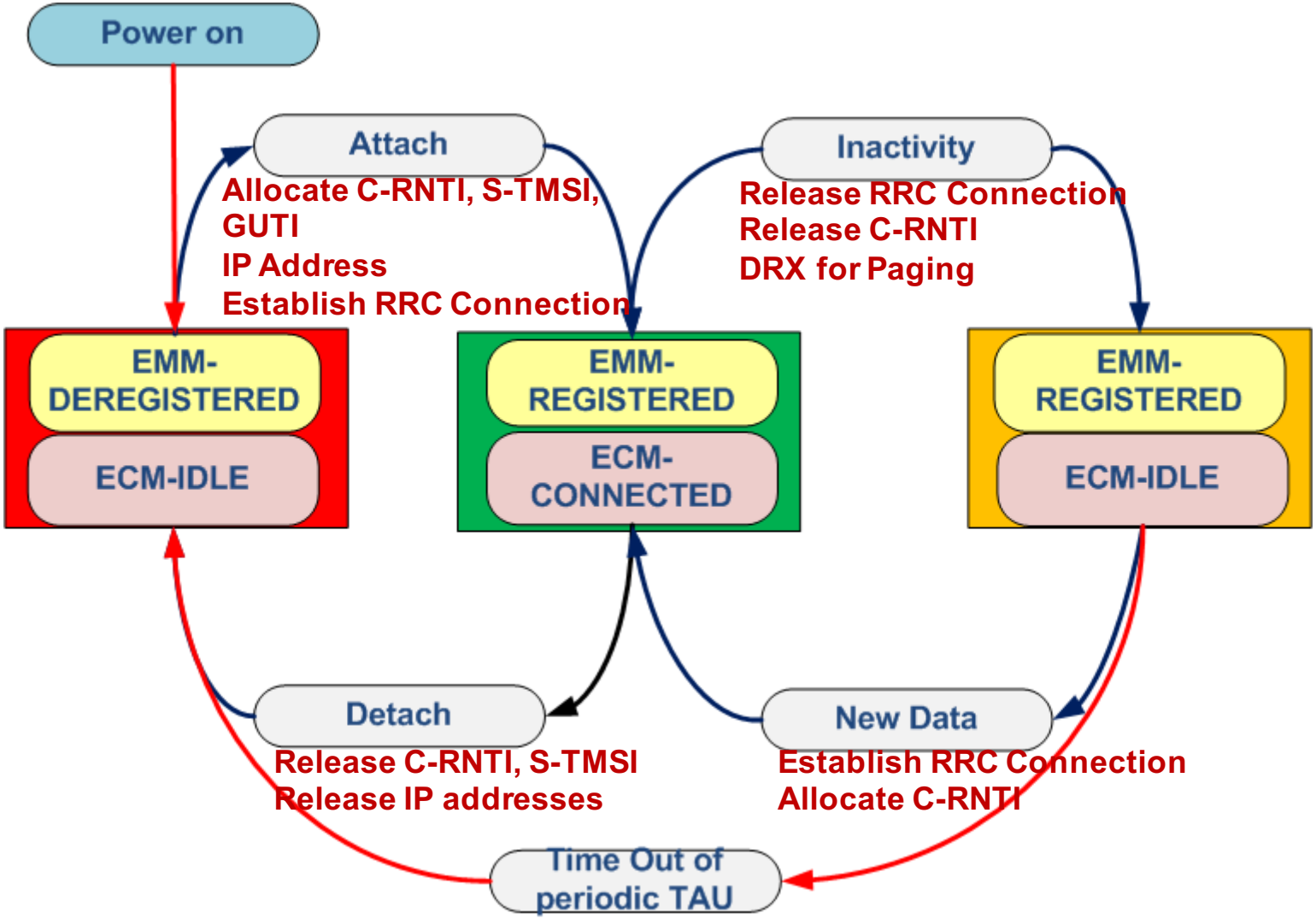
- Once a mobile device is switched on it always has at least a default bearer. In other words, it always has an IP address when it is switched on.
- To reflect this, the following two state machines are used in LTE/SAE



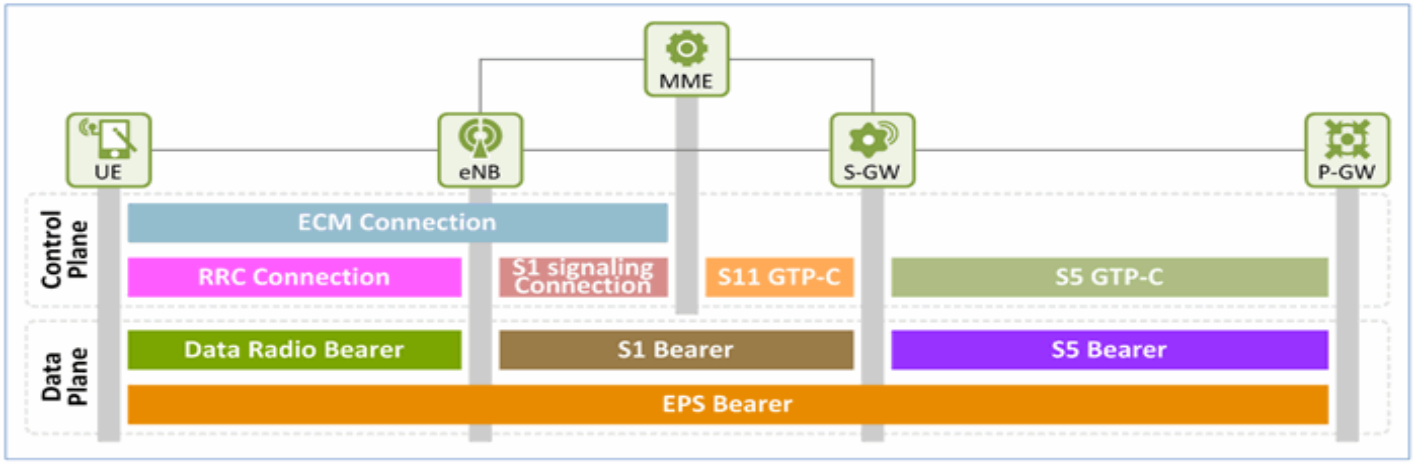
LTE Control states



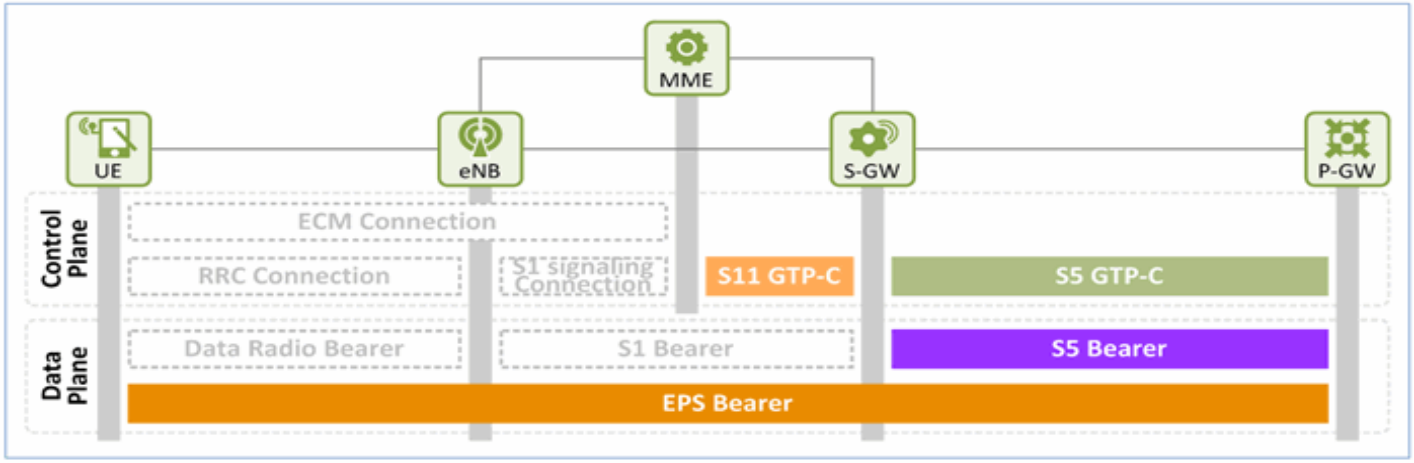
Mobility State Transition



Mobility States Transition



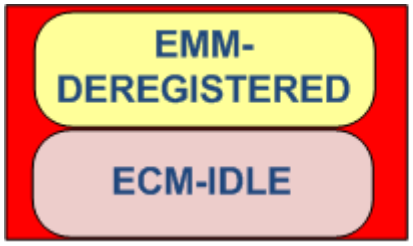
State C (EMM-Registered + ECM-Connected + RRC-Connected)



State D (EMM-Registered + ECM-Idle + RRC-Idle)

netwmanias.com

LTE states summary



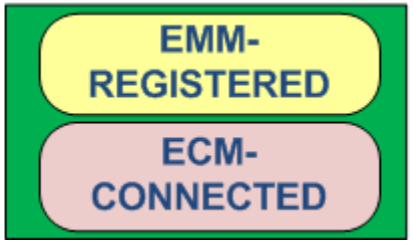
NW context:
None

Allocated IDs:
IMSI

UE Position:
Unknown to the NW

Mobility:
Cell selection
(i.e.PLMN selection)

UE Radio Activity:
None



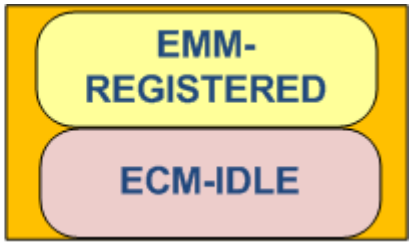
NW context:
Complete for
Data Tx/Rx

Allocated IDs:
IMSI, S-TMSI, C-RNTI
At least 1 IP address

UE Position:
Cell Level

Mobility:
Handover

UE Radio Activity:
DL no DRX
UL no DTX



NW context:
Security Context

Allocated IDs:
IMSI, S-TMSI
At least 1 IP address

UE Position:
Tracking Area

Mobility:
Cell re-selection

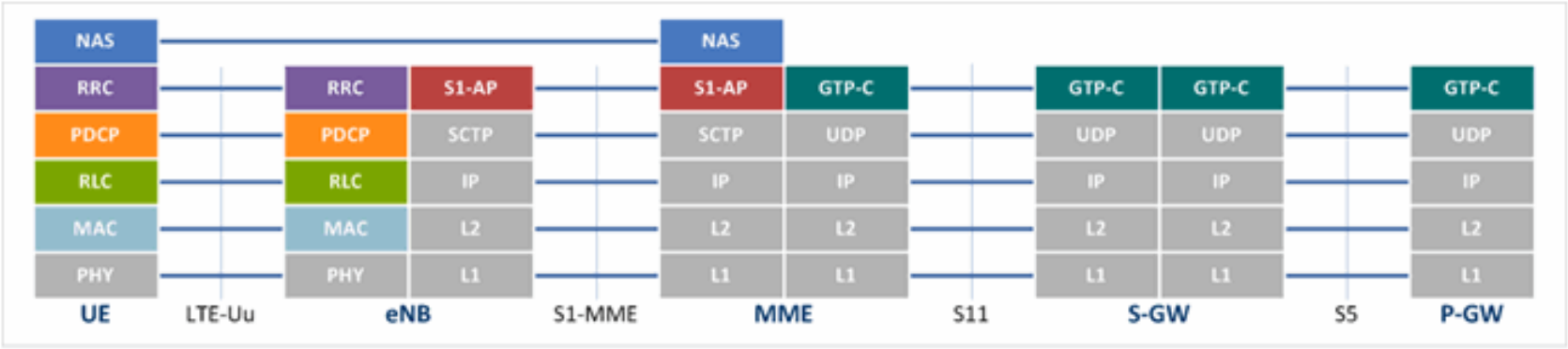
UE Radio Activity:
DL DRX or Paging
UL : none

Identities (in blue: allocated)

UE	eNodeB	MME	SGW	PGW	HSS
IMSI		IMSI	IMSI	IMSI	IMSI
GUTI		GUTI			
UE IP address		UE IP address		UE IP address	
	NB S1AP UE ID	NB S1AP UE ID			
	MME S1AP UE ID	MME S1AP UE ID			
APN in Use					
EPS Bearer ID	EPS Bearer ID	EPS Bearer ID	EPS Bearer ID	EPS Bearer ID	
DRB ID	DRB ID				
	E-RAB ID	E-RAB ID			
	S1 eNB TEID (DL)	S1 eNB TEID (DL)	S1 SGW TEID (UL)		
	S1 SGW TEID (UL)	S1 SGW TEID (UL)			
		S5 TEID (UL/DL)	S5 SGW TEID (DL)	S5 PGW TEID (UL)	
			S5 PGW TEID (UL)	S5 SGW TEID (DL)	

NAS procedures

NAS procedures



Non-Access Stratum (NAS)

- Protocol plan protocol at the MME and UE.
- Roughly, NAS features are classified into EPS Mobility Management (EMM) and EPS Connection Management (ECM)
  - Registration De-registration, Authentication
  - NAS Ciphering, NAS integrity
  - E2E Bearer setup, IP address allocation
  - Paging support
  - Mobility Management
  - UE initiated Attach/Detach, NW initiated Attach/Detach
  - Tracking Area Update procedure

S1AP protocol

- S1 Application Protocol (S1AP) provides the control plane signalling between the RAN and EPC.
  - The used interface is S1-MME which is located between eNB and MME.
  - The S1AP protocol provides transport function between UE and MME by offering NAS signalling transport.
  - Exchange general configuration messages between eNB and MME
  - Used by the MME to request the activation of specific functions at the eNB related to a UE connection
  - It delivers the initial UE context to the eNB to setup E-RAB(s) and manages modification or release of the UE context thereafter.
  - Used by the eNB to inform the MME about UE's state changes
  - Carries messages between the MME and UEs
- Each S1AP message includes the UE identity concerned by the message (except the first one exchanged between the eNB and MME: initial set up)
  - Relies on Stream Control Transmission Protocol (SCTP) => Reliable transport protocol
  - Appropriate for the transport of messages. TCP is flow-based

S1AP protocol

```
98   fd00::200          fd00::191          S1AP/…   240  InitialUEMessage, Attach request, PDN connectivity request
93   fd00::191          fd00::200          S1AP/…   128  DownlinkNASTransport, Identity request
82   fd00::200          fd00::191          S1AP/…   160  UplinkNASTransport, Identity response
57   fd00::191          fd00::200          S1AP/…   160  DownlinkNASTransport, Authentication request
52   fd00::200          fd00::191          S1AP/…   160  UplinkNASTransport, Authentication response
91   fd00::191          fd00::200          S1AP/…   144  DownlinkNASTransport, Security mode command
84   fd00::200          fd00::191          S1AP/…   168  UplinkNASTransport, Security mode complete
93   fd00::191          fd00::200          S1AP/…   136  DownlinkNASTransport, ESM information request
81   fd00::200          fd00::191          S1AP/…   204  UplinkNASTransport, ESM information response
```

```
tes on wire (1920 bits), 240 bytes captured (1920 bits) on interface 0
pture
ol Version 6, Src: fd00::200, Dst: fd00::191
Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
Protocol
tiatingMessage (0)
Message
eCode: id-initialUEMessage (12)
ity: ignore (1)

alUEMessage
tocolIEs: 5 items
Item 0: id-eNB-UE-S1AP-ID
▼ ProtocolIE-Field
    id: id-eNB-UE-S1AP-ID (8)
    criticality: reject (0)
  ▼ value
      ENB-UE-S1AP-ID: 103
Item 1: id-NAS-PDU
▼ ProtocolIE-Field
```

S1AP protocol

```
98   fd00::200          fd00::191          S1AP/…   240  InitialUEMessage, Attach request, PDN connectivity request
93   fd00::191          fd00::200          S1AP/…   128  DownlinkNASTransport, Identity request
82   fd00::200          fd00::191          S1AP/…   160  UplinkNASTransport, Identity response
57   fd00::191          fd00::200          S1AP/…   160  DownlinkNASTransport, Authentication request
52   fd00::200          fd00::191          S1AP/…   160  UplinkNASTransport, Authentication response
91   fd00::191          fd00::200          S1AP/…   144  DownlinkNASTransport, Security mode command
84   fd00::200          fd00::191          S1AP/…   168  UplinkNASTransport, Security mode complete
93   fd00::191          fd00::200          S1AP/…   136  DownlinkNASTransport, ESM information request
81   fd00::200          fd00::191          S1AP/…   204  UplinkNASTransport, ESM information response
```

```
tes on wire (1920 bits), 240 bytes captured (1920 bits) on interface 0
pture
ol Version 6, Src: fd00::200, Dst: fd00::191
Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
Protocol
tiatingMessage (0)
Message
eCode: id-initialUEMessage (12)
ity: ignore (1)

alUEMessage
tocolIEs: 5 items
Item 0: id-eNB-UE-S1AP-ID
▼ ProtocolIE-Field
    id: id-eNB-UE-S1AP-ID (8)
    criticality: reject (0)
  ▼ value
      ENB-UE-S1AP-ID: 103
Item 1: id-NAS-PDU
▼ ProtocolIE-Field
```

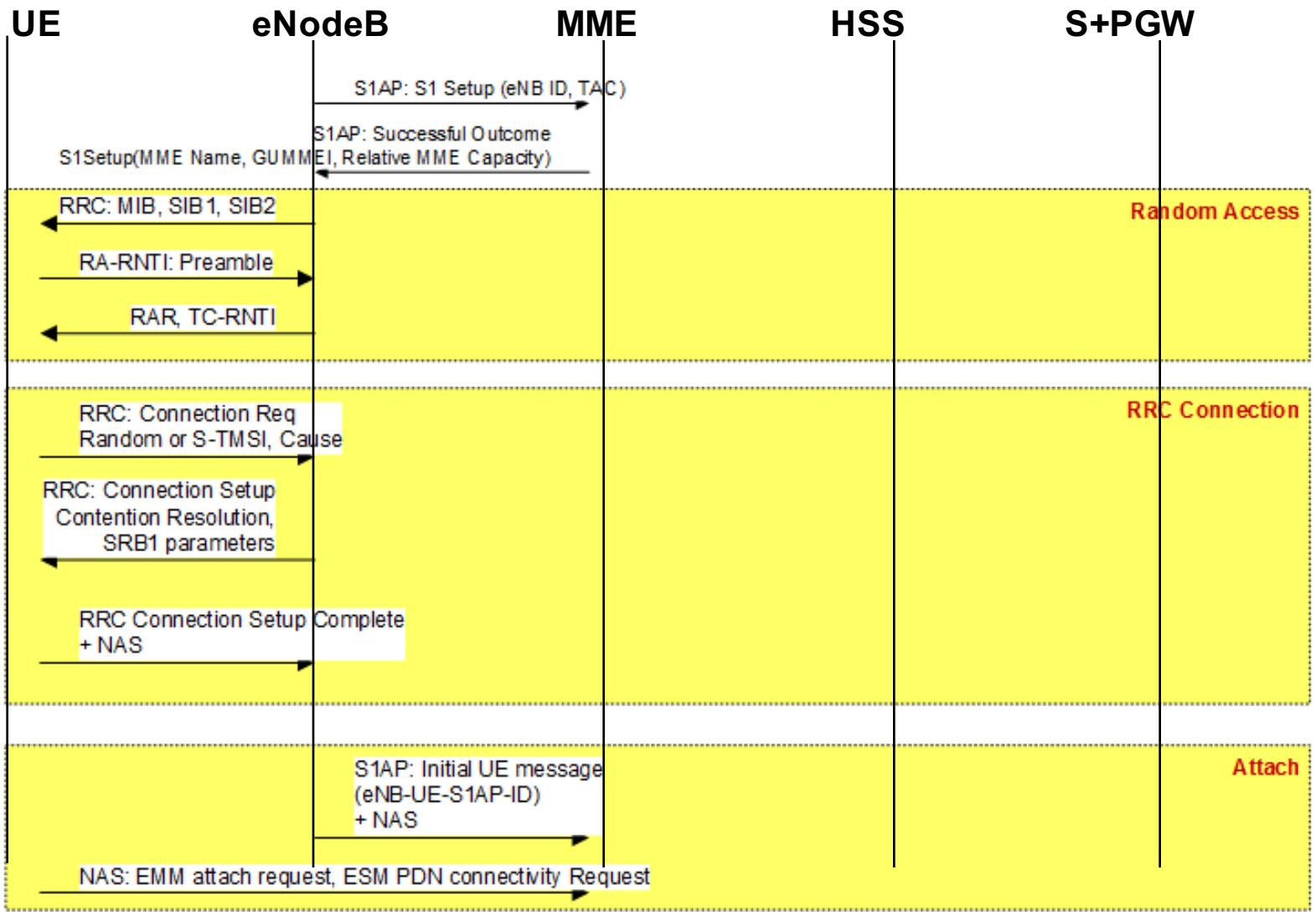
S1AP

```
 24 5.922987460   fd00::191           fd00::200           S1AP/…    284 InitialContextSetupRequest, Attach accept, Activate default EPS bearer conte
 25 5.923884481   fd00::200           fd00::191           S1AP      152 InitialContextSetupResponse
ream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
 Application Protocol
S1AP-PDU: initiatingMessage (0)
▼ initiatingMessage
     procedureCode: id-InitialContextSetup (9)
     criticality: reject (0)
   ▼ value
     ▼ InitialContextSetupRequest
       ▼ protocolIEs: 6 items
         ▼ Item 0: id-MME-UE-S1AP-ID
           ▼ ProtocolIE-Field
                id: id-MME-UE-S1AP-ID (0)
                criticality: reject (0)
             ▼ value
                  MME-UE-S1AP-ID: 1
         ▼ Item 1: id-eNB-UE-S1AP-ID
           ▼ ProtocolIE-Field
                id: id-eNB-UE-S1AP-ID (8)
                criticality: reject (0)
             ▼ value
                  ENB-UE-S1AP-ID: 103
         ▼ Item 2: id-uEaggregateMaximumBitrate
           ▶ ProtocolIE-Field
         ▼ Item 3: id-E-RABToBeSetupListCtxtSUReq
           ▶ ProtocolIE-Field
         ▼ Item 4: id-UESecurityCapabilities
           ▶ ProtocolIE-Field
         ▼ Item 5: id-SecurityKey
```

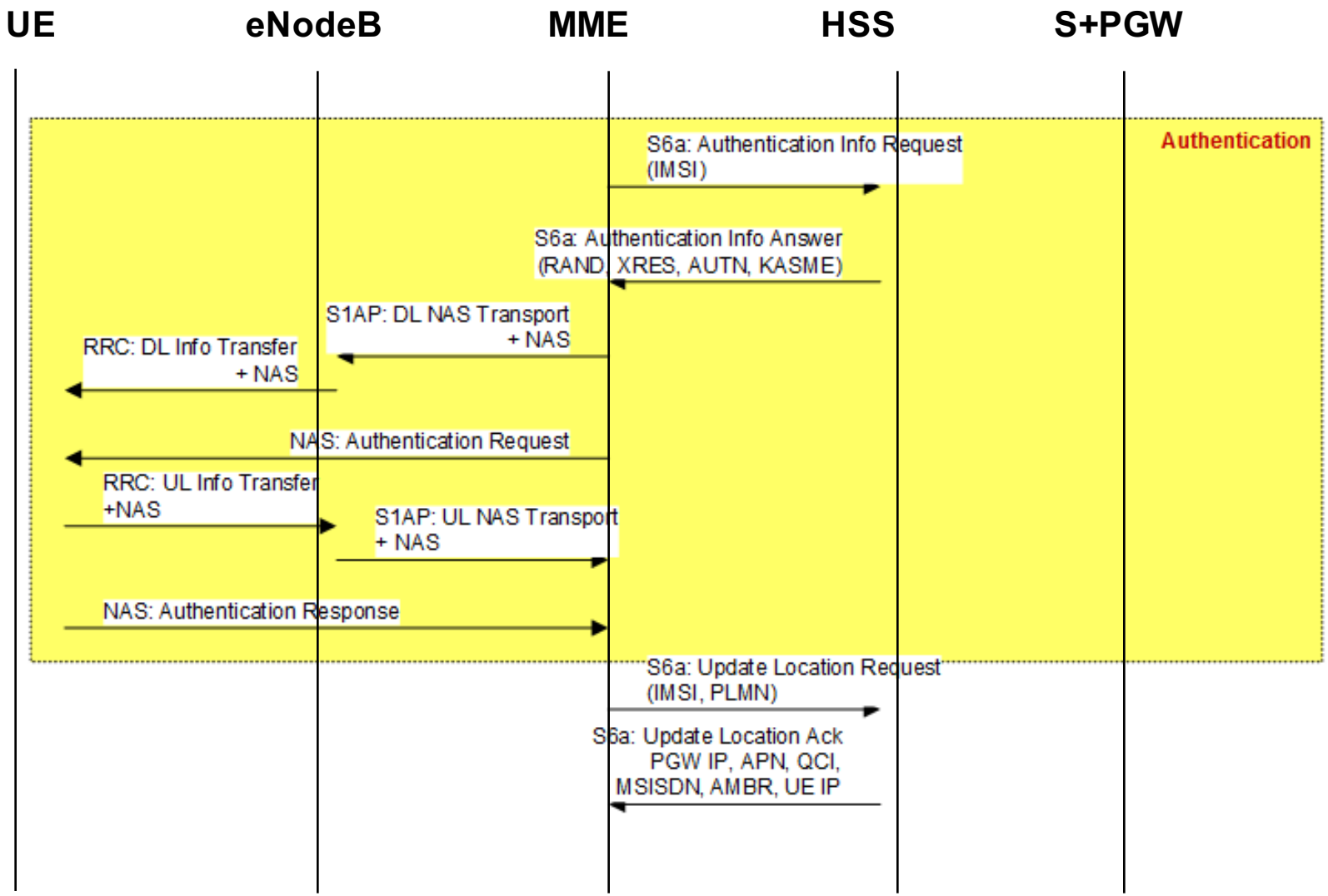
S1AP

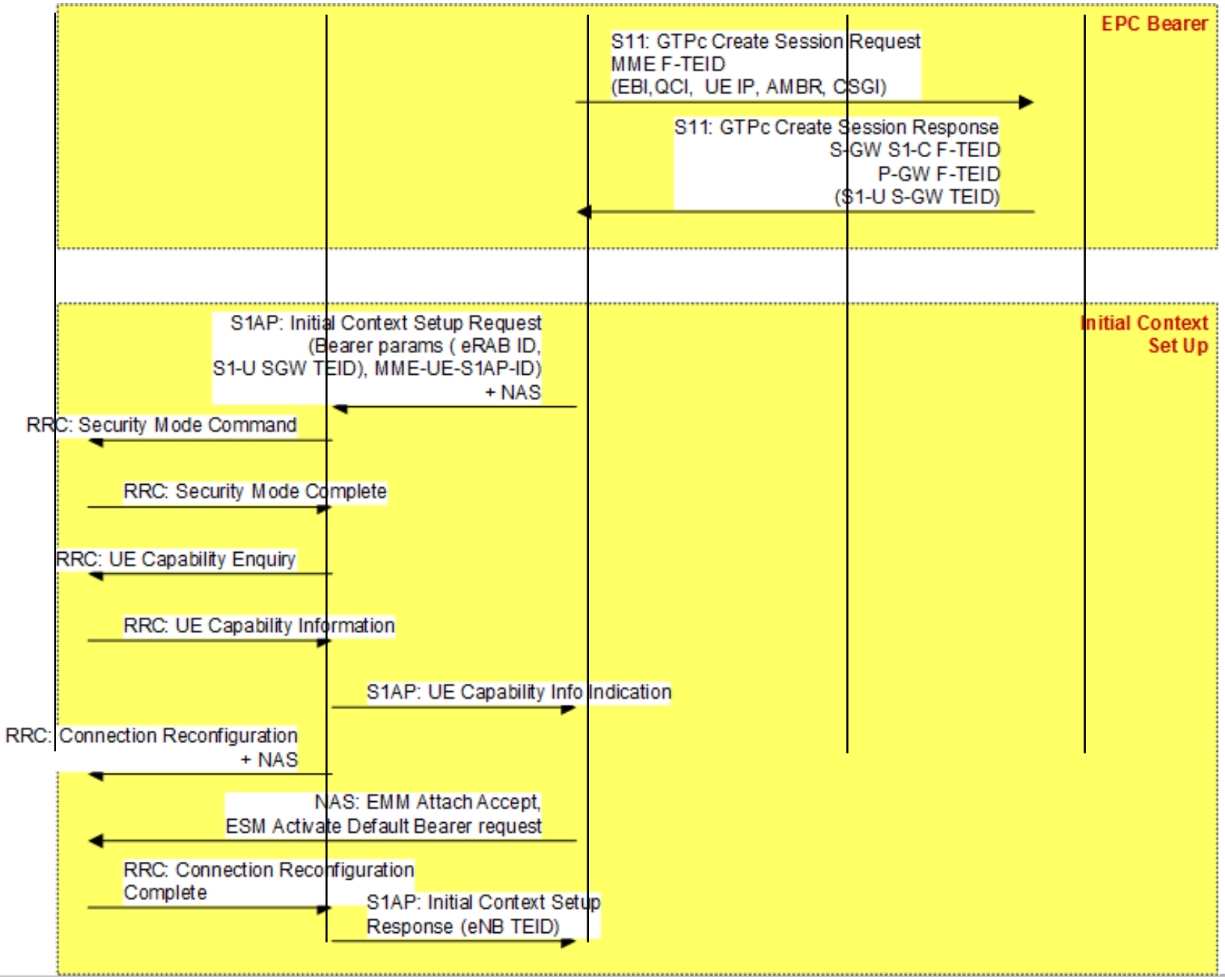
```
 24 5.922987460   fd00::191           fd00::200           S1AP/…    284 InitialContextSetupRequest, Attach accept, Activate default EPS bearer conte
 25 5.923884481   fd00::200           fd00::191           S1AP      152 InitialContextSetupResponse
ream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
 Application Protocol
S1AP-PDU: initiatingMessage (0)
▼ initiatingMessage
     procedureCode: id-InitialContextSetup (9)
     criticality: reject (0)
   ▼ value
     ▼ InitialContextSetupRequest
       ▼ protocolIEs: 6 items
         ▼ Item 0: id-MME-UE-S1AP-ID
           ▼ ProtocolIE-Field
                id: id-MME-UE-S1AP-ID (0)
                criticality: reject (0)
             ▼ value
                  MME-UE-S1AP-ID: 1
         ▼ Item 1: id-eNB-UE-S1AP-ID
           ▼ ProtocolIE-Field
                id: id-eNB-UE-S1AP-ID (8)
                criticality: reject (0)
             ▼ value
                  ENB-UE-S1AP-ID: 103
         ▼ Item 2: id-uEaggregateMaximumBitrate
           ▶ ProtocolIE-Field
         ▼ Item 3: id-E-RABToBeSetupListCtxtSUReq
           ▶ ProtocolIE-Field
         ▼ Item 4: id-UESecurityCapabilities
           ▶ ProtocolIE-Field
         ▼ Item 5: id-SecurityKey
```

LTE UE Attach

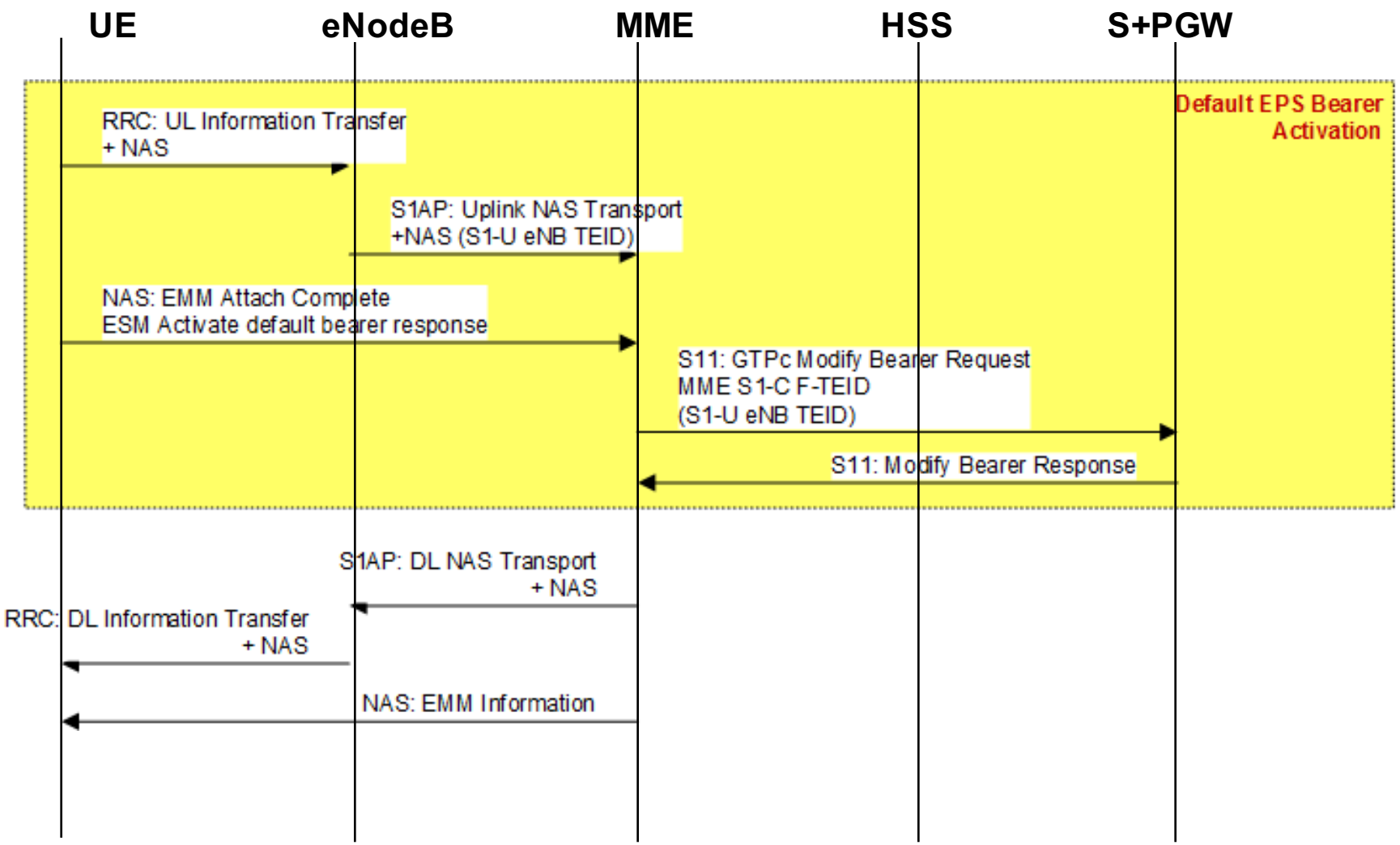


LTE UE Attach

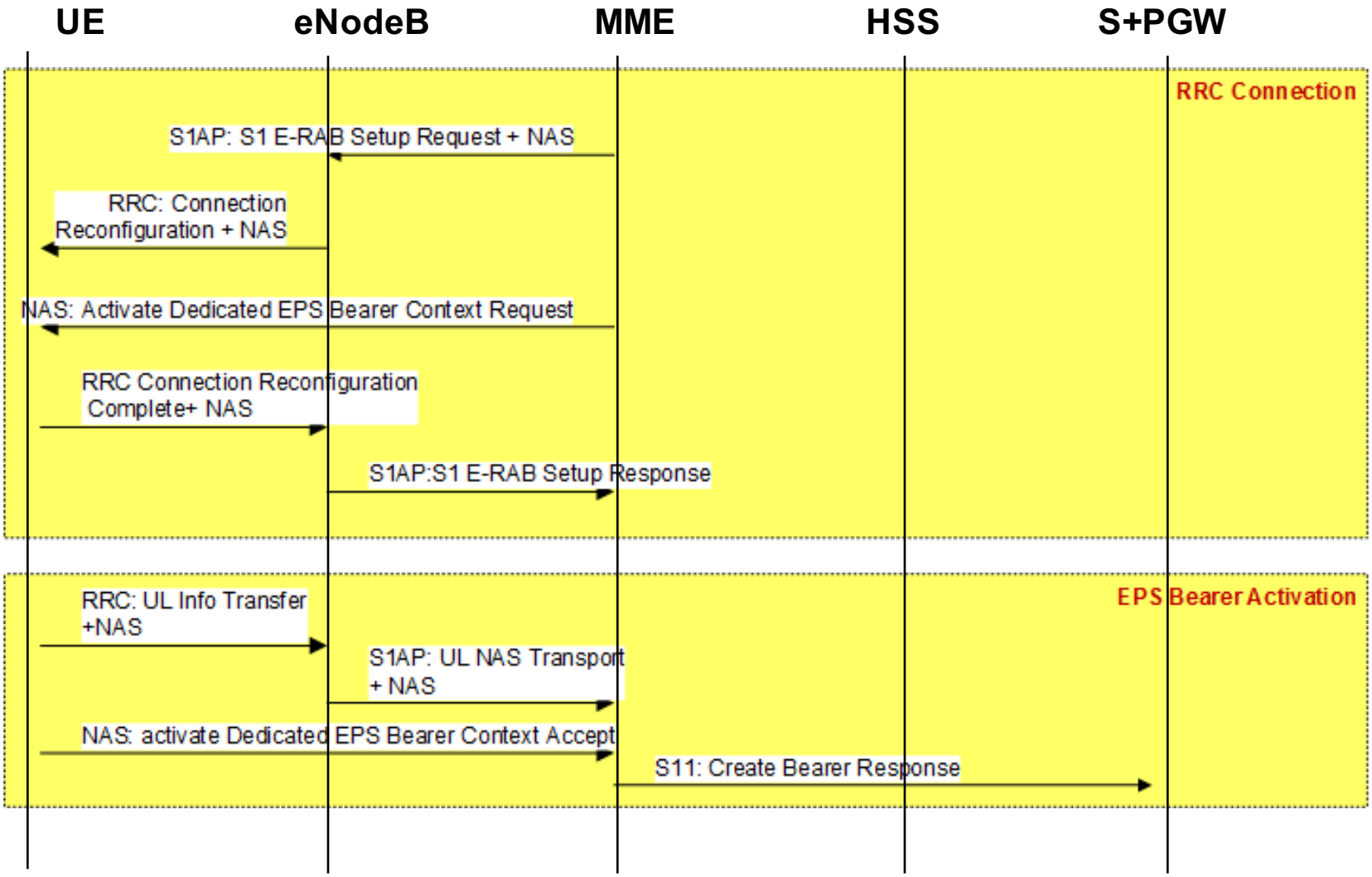



EPC Bearer
S11: GTPc Create Session Request
MME F-TEID
(EBI,QCI, UE IP, AMBR, CSGI)
S11: GTPc Create Session Response
S-GW S1-C F-TEID
P-GW F-TEID
(S1-U S-GW TEID)
Initial Context Set Up
S1AP: Initial Context Setup Request
(Bearer params (eRAB ID,
S1-U SGW TEID), MME-UE-S1AP-ID)
+ NAS
RRC: Security Mode Command
RRC: Security Mode Complete
RRC: UE Capability Enquiry
RRC: UE Capability Information
S1AP: UE Capability Info Indication
RRC: Connection Reconfiguration
+ NAS
NAS: EMM Attach Accept,
ESM Activate Default Bearer request
RRC: Connection Reconfiguration
Complete
S1AP: Initial Context Setup
Response (eNB TEID)

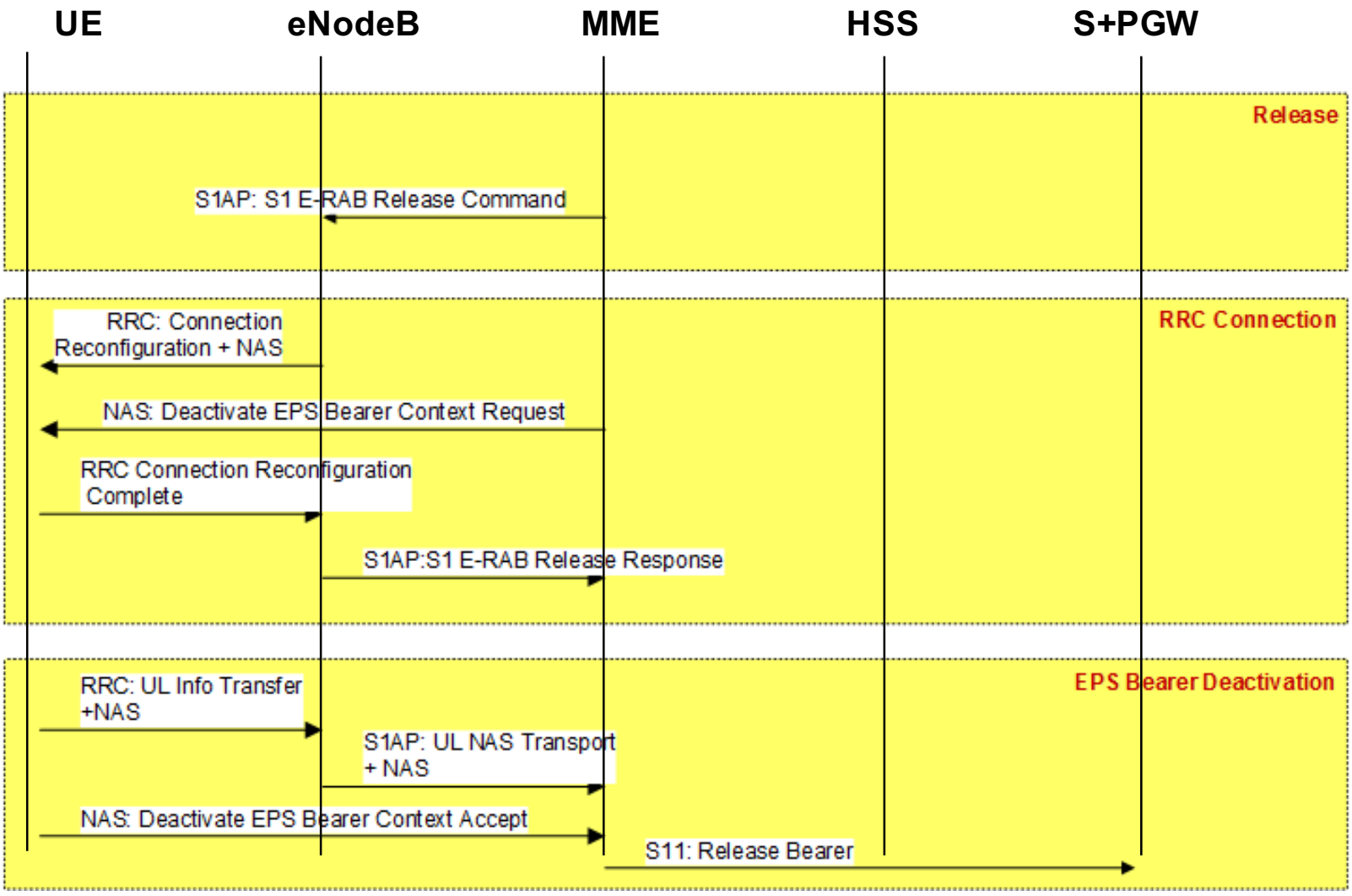
LTE UE Attach



Dedicated bearer



Detach


UE
eNodeB
MME
HSS
S+PGW
Release
S1AP: S1 E-RAB Release Command
RRC Connection
RRC: Connection Reconfiguration + NAS
NAS: Deactivate EPS Bearer Context Request
RRC Connection Reconfiguration Complete
S1AP:S1 E-RAB Release Response
EPS Bearer Deactivation
RRC: UL Info Transfer +NAS
S1AP: UL NAS Transport + NAS
NAS: Deactivate EPS Bearer Context Accept
S11: Release Bearer

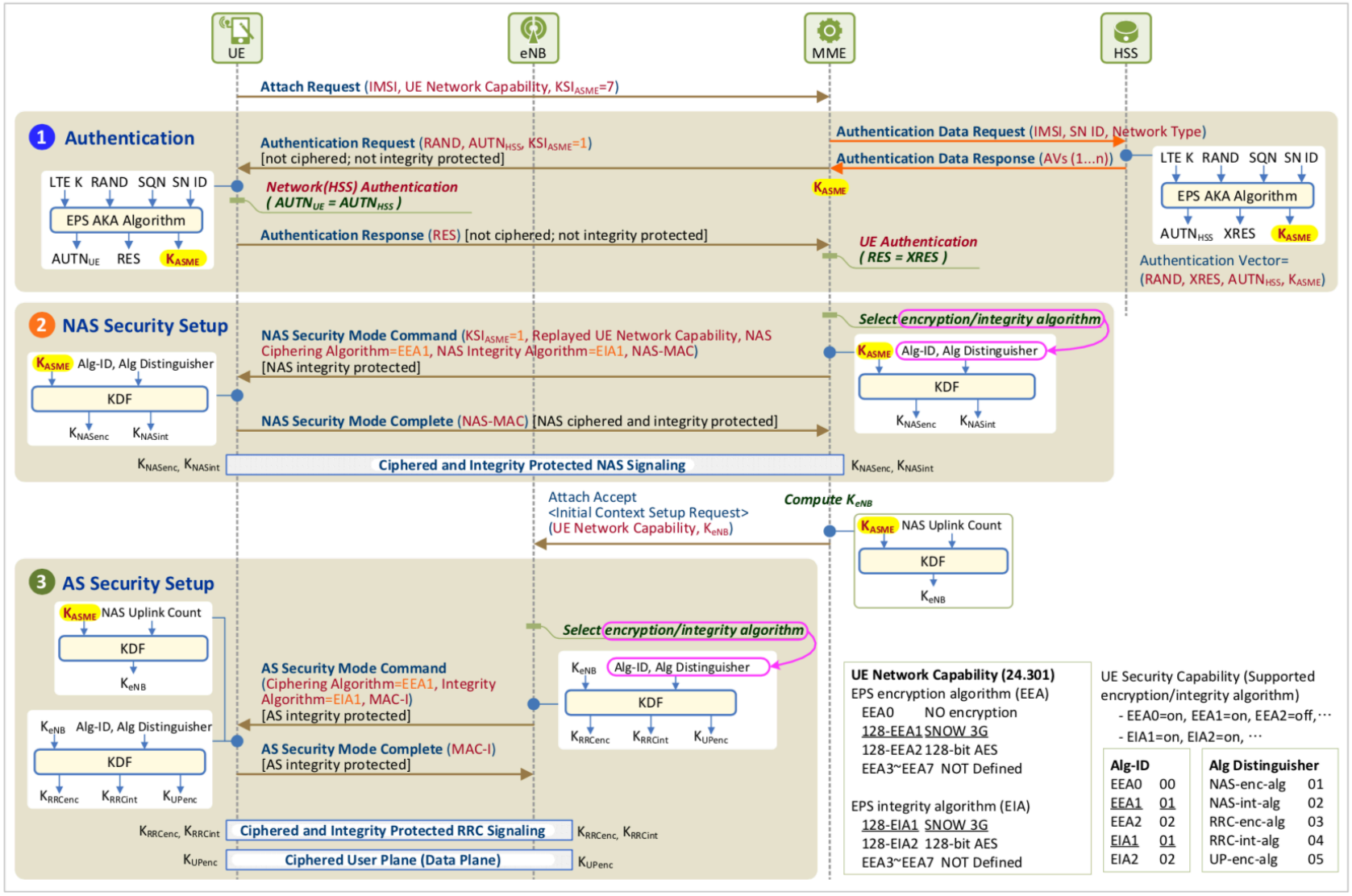
Initial UE eNB->MME

Initial UE Message (eNB UE S1AP ID, NAS-PDU, TAI, ECGI, RRC Establishment Cause)

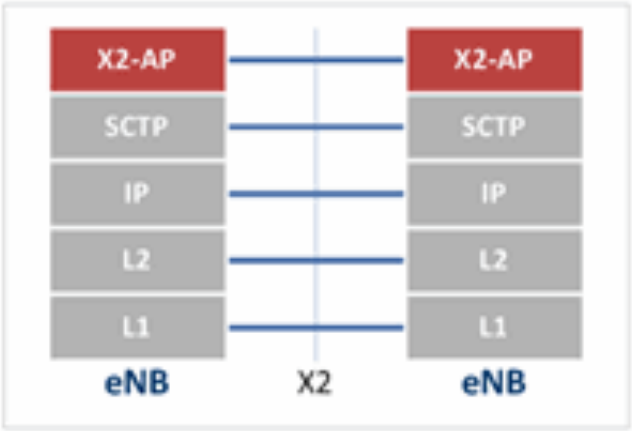
- **eNB UE S1AP ID:** ID identifying UEs in an eNB over S1-MME interface (Uplink)
- **NAS-PDU:** a NAS message (**Attach Request**)
- **TAI:** shows the TA a UE is located in
- **ECGI:** shows the cell a UE is located in
- **RRC Establishment Cause = mo-Signaling:** indicates the signaling was generated by a UE

Security details

Security details

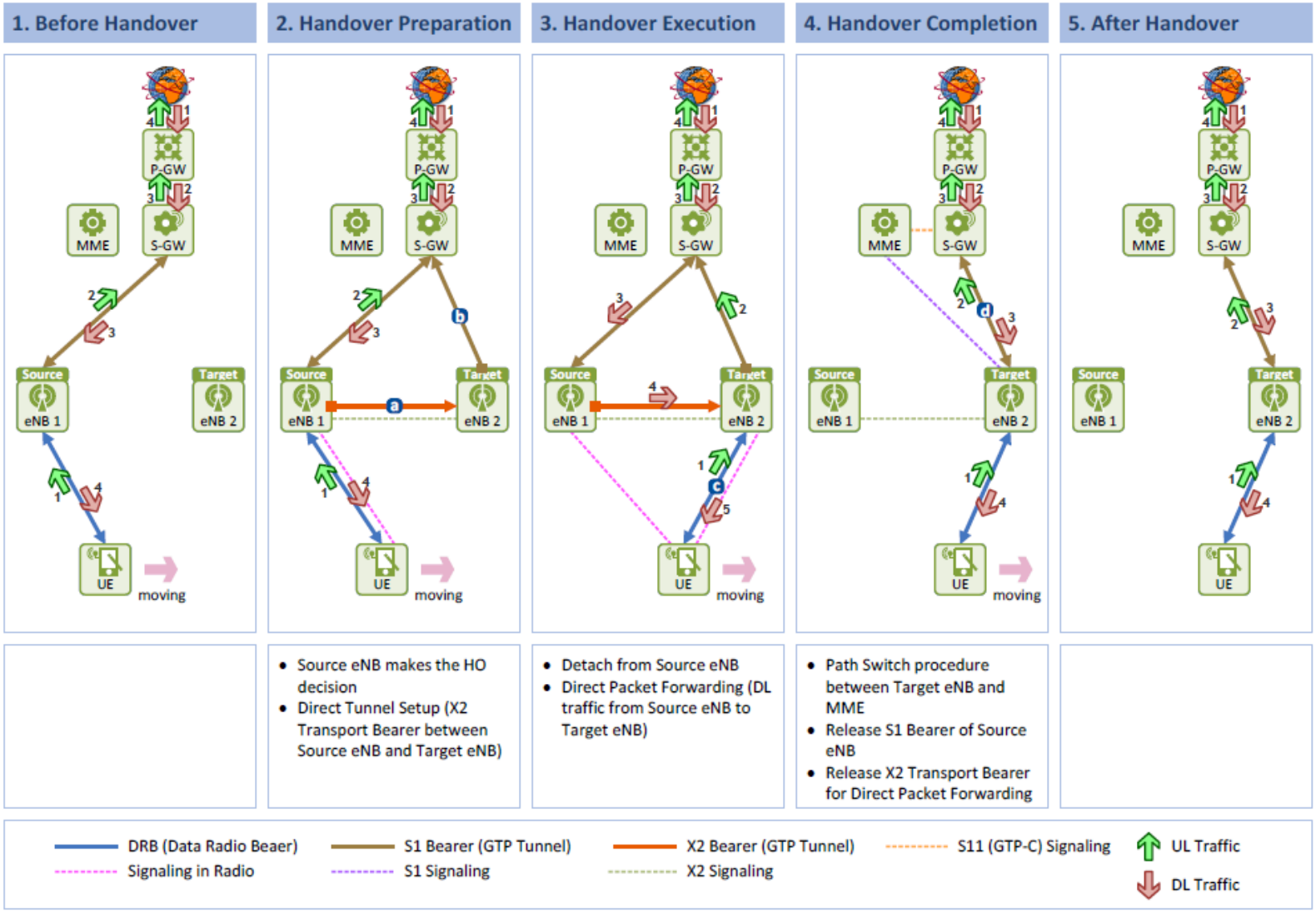


X2 interface

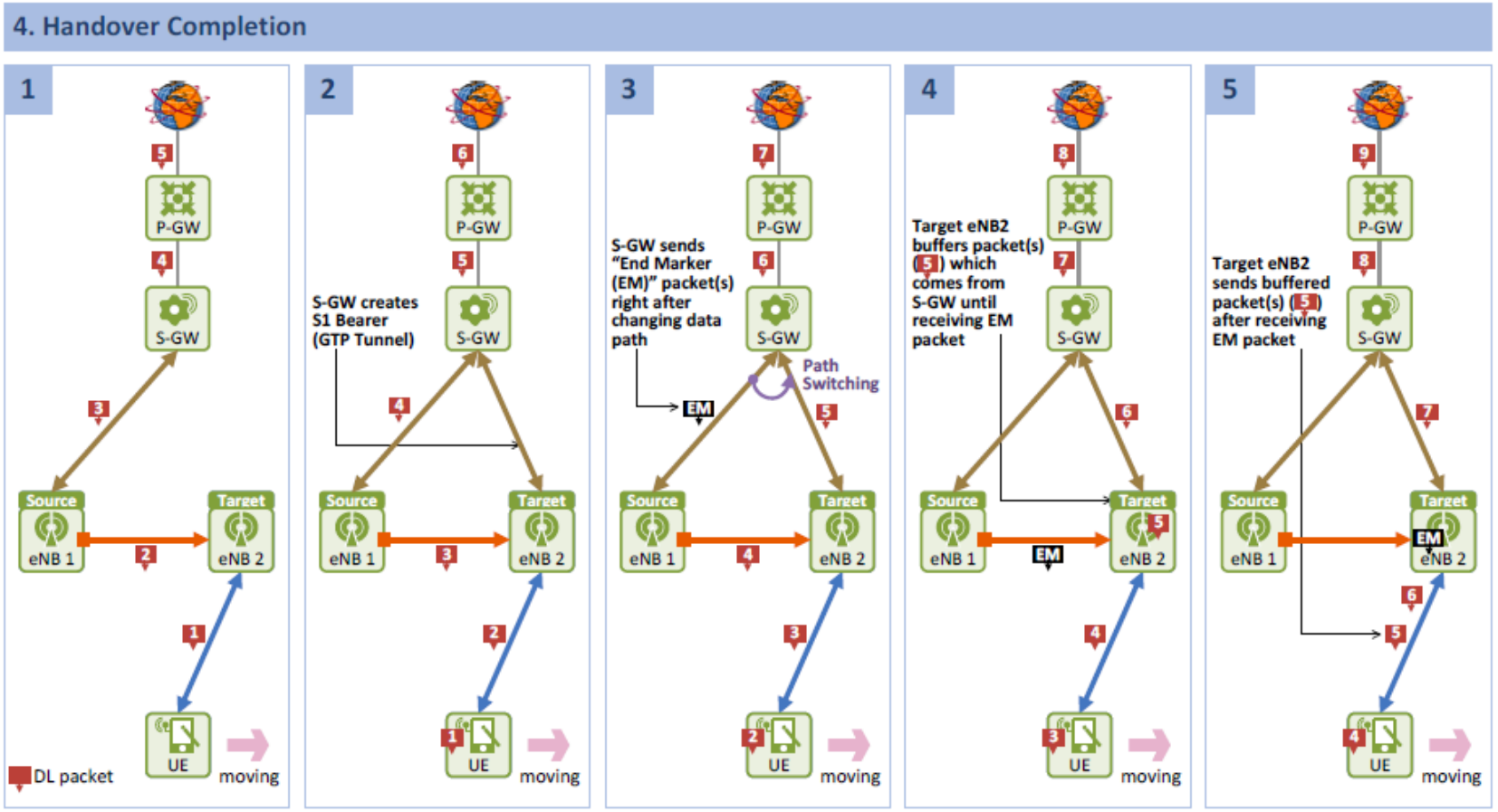


- X2AP is a control protocol found between eNBs on the X2 control plane.
  - Supports UE mobility and Self-Organization Network (SON) functions within the E-UTRAN.
  - Provides functions such as user data forwarding, transfer of SN status and UE context release.
- For SON functions, eNBs exchange resource status information, traffic load information and eNB configuration update information, and coordinate each other to adjust mobility parameters using the X2AP protocol.

X2 Handover


1. Before Handover
2. Handover Preparation
3. Handover Execution
4. Handover Completion
5. After Handover
P-GW
S-GW
MME
Source
Target
eNB 1
eNB 2
UE
moving
• Source eNB makes the HO decision
• Direct Tunnel Setup (X2 Transport Bearer between Source eNB and Target eNB)
• Detach from Source eNB
• Direct Packet Forwarding (DL traffic from Source eNB to Target eNB)
• Path Switch procedure between Target eNB and MME
• Release S1 Bearer of Source eNB
• Release X2 Transport Bearer for Direct Packet Forwarding
DRB (Data Radio Beaer)
Signaling in Radio
S1 Bearer (GTP Tunnel)
S1 Signaling
X2 Bearer (GTP Tunnel)
X2 Signaling
S11 (GTP-C) Signaling
UL Traffic
DL Traffic

X2 Handover


4. Handover Completion
1
2
3
4
5
P-GW
S-GW
Source
Target
eNB 1
eNB 2
UE
moving
DL packet
S-GW creates S1 Bearer (GTP Tunnel)
S-GW sends "End Marker (EM)" packet(s) right after changing data path
EM
Path Switching
Target eNB2 buffers packet(s) (5) which comes from S-GW until receiving EM packet
Target eNB2 sends buffered packet(s) (5) after receiving EM packet