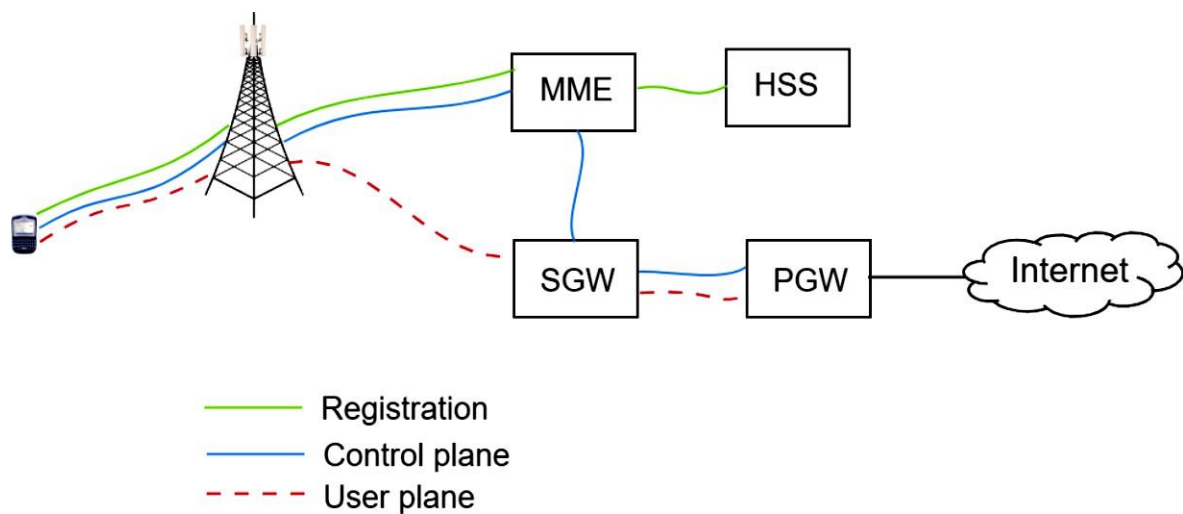


IN LAB

Files Requirement:

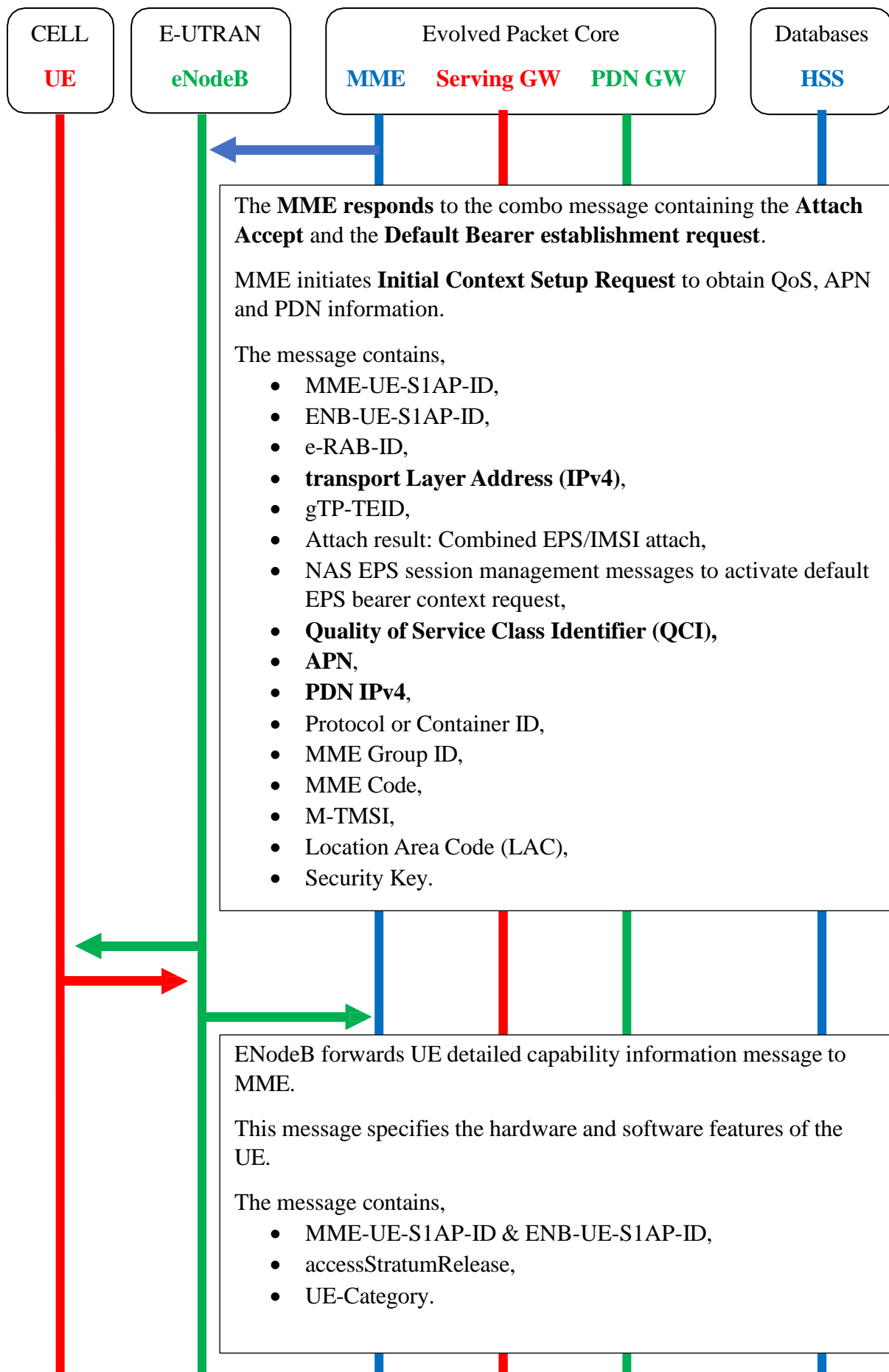
- During Experiment 1, **.pcap** files were generated for CN and eNB in Step 8 and Step 14.
- Experiment 2, Step 1 and 2 from will be informative.

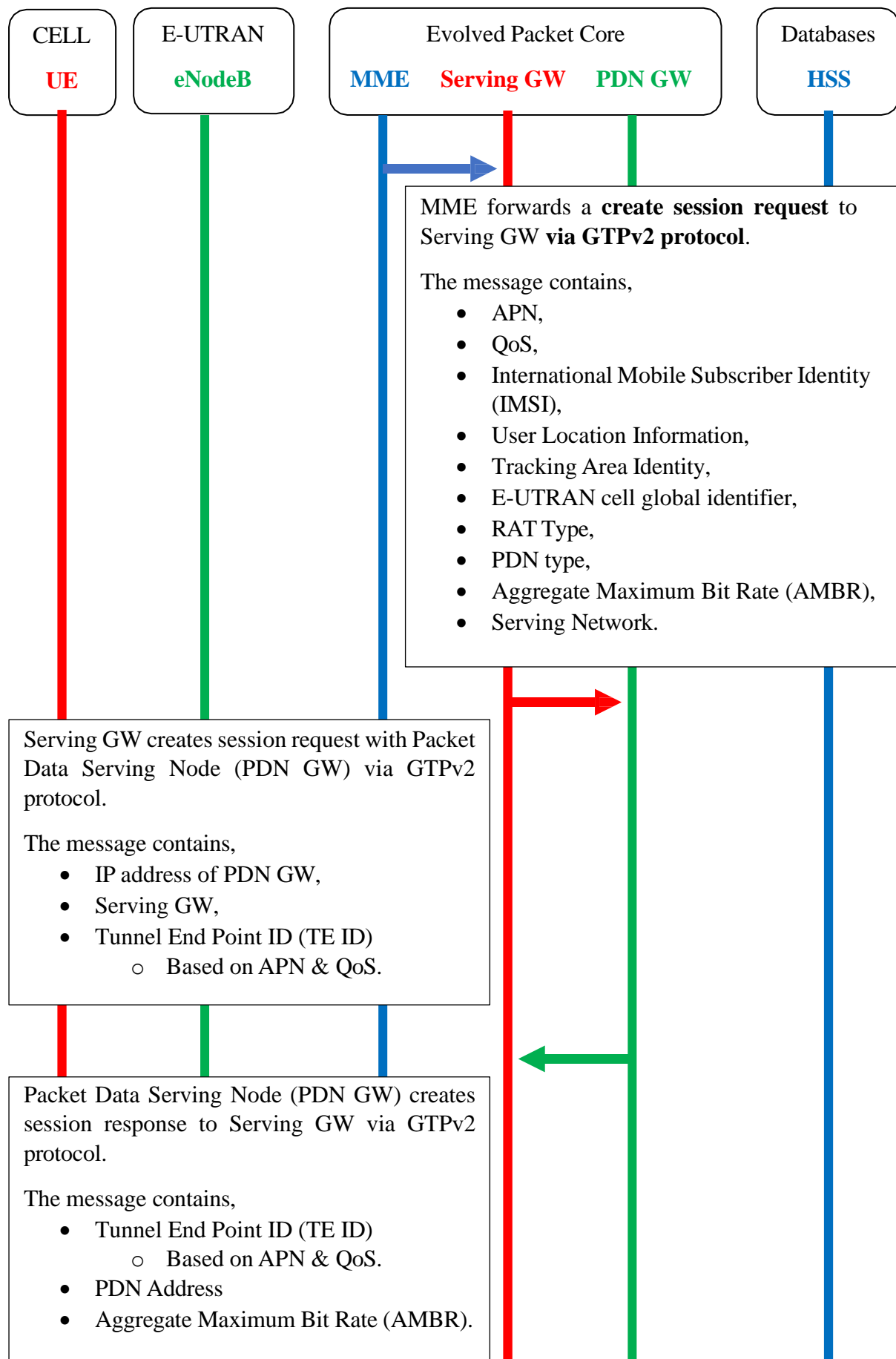
Let's analyze the UE registration messages between eNodeB, MME and HSS to enable LTE session.

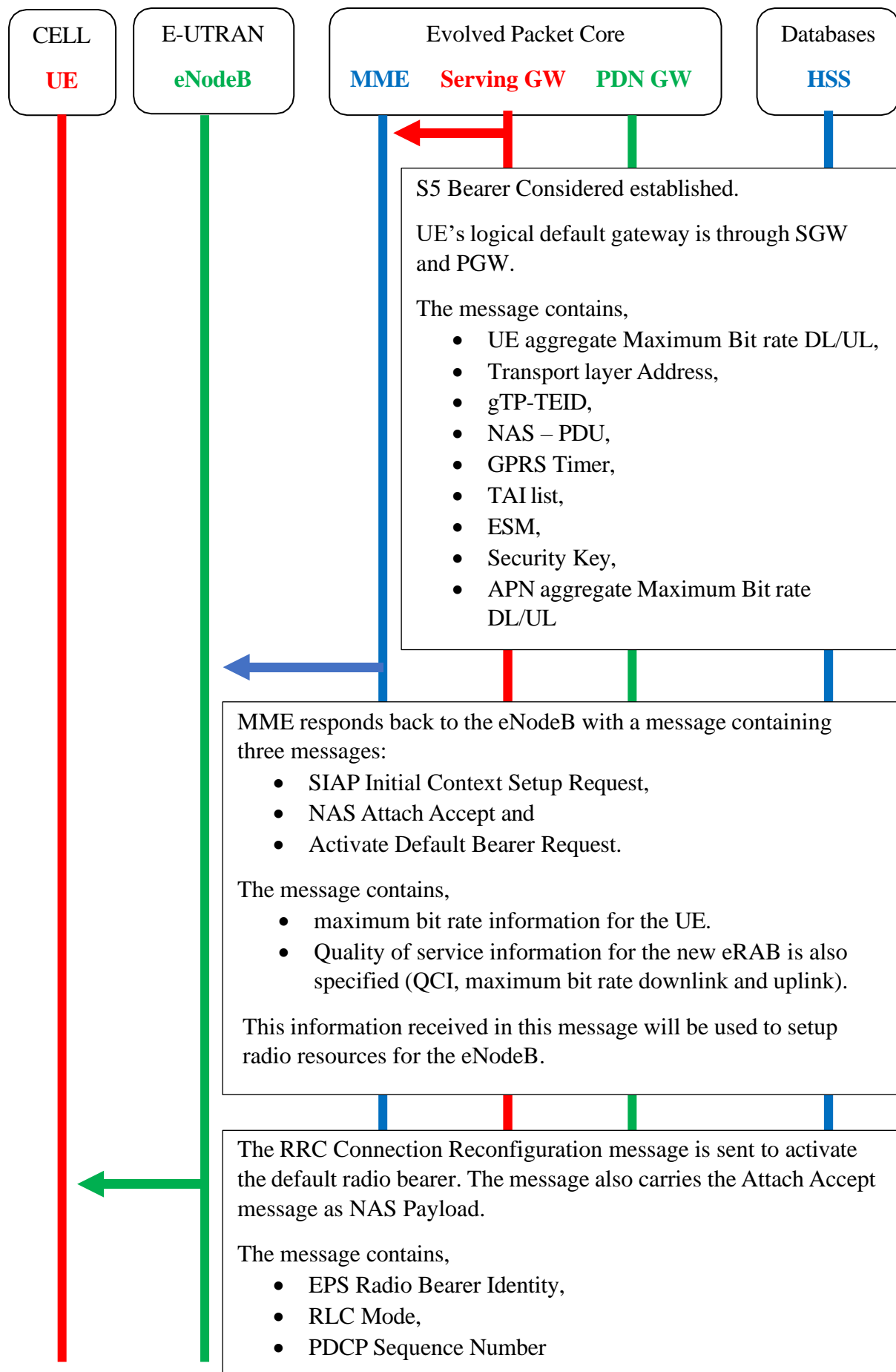


Control Plane

In this experiment we will explore the process and communication to establish data service and assign an IP address to the UE as well as QoS parameters.





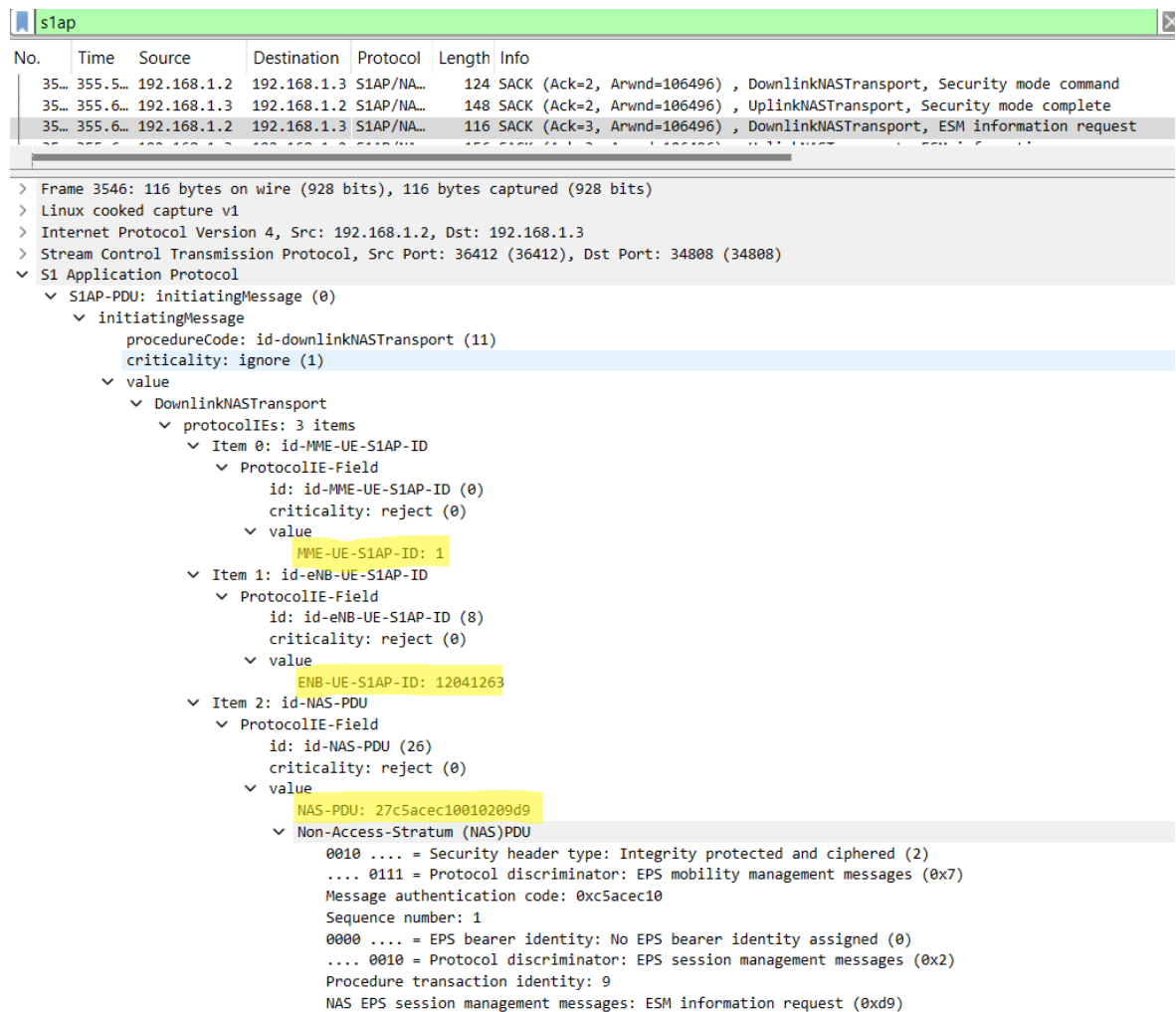


Open .pcap file using Wireshark.

1. In Wireshark after applying slap filter, Downlink NAS Transport to view ESM information request.

NOTE: At Step 1, take a screenshot and attach it.

Highlight the initial message fields



2. In Wireshark after applying slap filter, Uplink NAS Transport to view ESM information response.

NOTE: At Step 2, take a screenshot and attach it.

Highlight the initial message fields

slap

No.	Time	Source	Destination	Protocol	Length	Info
35...	355.6...	192.168.1.3	192.168.1.2	S1AP/NA...	148	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete
35...	355.6...	192.168.1.2	192.168.1.3	S1AP/NA...	116	SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, ESM information request
35...	355.6...	192.168.1.3	192.168.1.2	S1AP/NA...	156	SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, ESM information response

- S1 Application Protocol
 - S1AP-PDU: initiatingMessage (0)
 - initiatingMessage
 - procedureCode: id-uplinkNASTransport (13)
 - criticality: ignore (1)
 - value
 - UplinkNASTransport
 - protocolIEs: 5 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: 12041263
 - Item 2: id-NAS-PDU
 - ProtocolIE-Field
 - id: id-NAS-PDU (26)
 - criticality: reject (0)
 - value
 - NAS-PDU: 2790897ba0010209da280e086368616e64686172046c616273
 - Non-Access-Stratum (NAS)PDU
 - 0010 = Security header type: Integrity protected and ciphered (2)
 - 0111 = Protocol discriminator: EPS mobility management messages (0x7)
 - Message authentication code: 0x90897ba0
 - Sequence number: 1
 - 0000 = EPS bearer identity: No EPS bearer identity assigned (0)
 - 0010 = Protocol discriminator: EPS session management messages (0x2)
 - Procedure transaction identity: 9
 - NAS EPS session management messages: ESM information response (0xda)
 - Access Point Name
 - Element ID: 0x28
 - Length: 14
 - APN: chandhar.labs
 - Item 3: id-EUTRAN-CGI
 - ProtocolIE-Field
 - id: id-EUTRAN-CGI (100)
 - criticality: ignore (1)
 - value
 - EUTRAN-CGI
 - plMNidentity: 02f829
 - Mobile Country Code (MCC): France (208)
 - Mobile Network Code (MNC): Unknown (92)
 - 0000 0000 1110 0000 0001 0000 0000 = cell-ID: 0x00e0100
 - Item 4: id-TAI
 - ProtocolIE-Field
 - id: id-TAI (67)
 - criticality: ignore (1)
 - value
 - TAI
 - plMNidentity: 02f829
 - Mobile Country Code (MCC): France (208)
 - Mobile Network Code (MNC): Unknown (92)
 - tAC: 1 (0x0001)

3. In Wireshark view the message details of Initial Context Setup Request, Attach accept, Activate default EPS bearer context request communicated via slap protocol.

NOTE: At Step 3, take a screenshot and attach it.

Identify the IP address of mobile.

6 MARKS

Highlight the initial message fields

2 MARKS

Page | 11

slap

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|----------|-------------|-------------|------------|--------|--|
| 35... | 355.5... | 192.168.1.2 | 192.168.1.3 | S1AP/NA... | 124 | SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command |
| 35... | 355.6... | 192.168.1.3 | 192.168.1.2 | S1AP/NA... | 148 | SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete |
| 35... | 355.6... | 192.168.1.2 | 192.168.1.3 | S1AP/NA... | 116 | SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, ESM information request |
| 35... | 355.6... | 192.168.1.3 | 192.168.1.2 | S1AP/NA... | 156 | SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, ESM information response |
| 35... | 355.6... | 192.168.1.2 | 192.168.1.3 | S1AP/NA... | 264 | SACK (Ack=4, Arwnd=106496) , InitialContextSetupRequest, Attach accept, Activate def |

- Item 1: id-eNB-UE-S1AP-ID
 - ProtocolIE-Field
 - id: id-eNB-UE-S1AP-ID (8)
 - criticality: reject (0)
 - value
 - eNB-UE-S1AP-ID: 12041263
- Item 2: id-uEAggregateMaximumBitrate
 - ProtocolIE-Field
 - id: id-uEAggregateMaximumBitrate (66)
 - criticality: reject (0)
 - value
 - UEAggregateMaximumBitrate
 - uEAggregateMaximumBitRateDL: 100000000bits/s
 - uEAggregateMaximumBitRateUL: 500000000bits/s
- Item 3: id-E-RABToBeSetupListCtxtSUReq
 - ProtocolIE-Field
 - id: id-E-RABToBeSetupListCtxtSUReq (24)
 - criticality: reject (0)
 - value
 - E-RABToBeSetupListCtxtSUReq: 1 item
 - Item 0: id-E-RABToBeSetupItemCtxtSUReq
 - ProtocolIE-SingleContainer
 - id: id-E-RABToBeSetupItemCtxtSUReq (52)
 - criticality: reject (0)
 - value
 - E-RABToBeSetupItemCtxtSUReq
 - e-RAB-ID: 5
 - e-RABlevelQoSParameters
 - qCI: 9
 - allocationRetentionPriority
 - priorityLevel: no-priority (15)
 - pre-emptionCapability: shall-not-trigger-pre-emption (0)
 - pre-emptionVulnerability: not-pre-emptable (0)
 - transportLayerAddress: c0a80102 [bit length 32, 1100 0000 1010 1000 0000 0001 0000 0010 d
 - transportLayerAddress(IPv4): 192.168.1.2
 - GTP-TEID: 00000001
 - transportLayerAddress(IPv4): 192.168.1.2
 - GTP-TEID: 00000001
- NAS-PDU: 271b2941040207420221062002f8290001002f5209c101090e086368616e64686172046c61627305010c0101025e04fefe9e6c270d80000d0408080
- Non-Access-Stratum (NAS)PDU
 - 0010 = Security header type: Integrity protected and ciphered (2)
 - 0111 = Protocol discriminator: EPS mobility management messages (0x7)
 - Message authentication code: 0x1b294104
 - Sequence number: 2
 - 0000 = Security header type: Plain NAS message, not security protected (0)
 - 0111 = Protocol discriminator: EPS mobility management messages (0x7)
 - NAS EPS Mobility Management Message Type: Attach accept (0x42)
 - 0000 = Spare half octet: 0
 - 0... = Spare bit(s): 0x00
 -010 = Attach result: Combined EPS/IMSI attach (2)
 - GPRS Timer - T3412 value
 - GPRS Timer: 1 min
 - 001. = Unit: value is incremented in multiples of 1 minute (1)
 - ...0 0001 = Timer value: 1
 - Tracking area identity list - TAI list
 - Length: 6
 - 0... = Spare bit(s): 0x00
 - .01. = Type of list: list of TACs belonging to one PLMN, with consecutive TAC values (1)
 - ...0 0000 = Number of elements: 0 [+1 = 1 element(s)]
 - Mobile Country Code (MCC): France (208)
 - Mobile Network Code (MNC): Unknown (92)
 - Tracking area code(TAC): 1
 - ESM message container
 - Length: 47
 - ESM message container contents: 5209c101090e086368616e64686172046c61627305010c0101025e04fefe9e6c270d80000d0408080800100:
 - 0101 = EPS bearer identity: EPS bearer identity value 5 (5)
 - 0010 = Protocol discriminator: EPS session management messages (0x2)
 - Procedure transaction identity: 9

```

Procedure transaction identity: 9
NAS EPS session management messages: Activate default EPS bearer context request (0xc1)
✓ EPS quality of service
  Length: 1
  Quality of Service Class Identifier (QCI): QCI 9 (9)
✓ Access Point Name
  Length: 14
  APN: chandhar.labs
✓ PDN address
  Length: 5
  0000 0... = Spare bit(s): 0x00
  PDN type: IPv4 (1)
  PDN IPv4: 12.1.1.2
✓ APN aggregate maximum bit rate
  Element ID: 0x5e
  Length: 4
  APN-AMBR for downlink: 8640 kbps
  APN-AMBR for uplink: 8640 kbps
  APN-AMBR for downlink (extended): 100 Mbps
  Total APN-AMBR for downlink: 100.000 Mbps
  APN-AMBR for uplink (extended): 50 Mbps
  Total APN-AMBR for uplink: 50.000 Mbps
✓ Protocol Configuration Options
  Element ID: 0x27
  Length: 13
  [Link direction: Network to MS (1)]
  1... .... = Extension: True
  .... .000 = Configuration Protocol: PPP for use with IP PDP type or IP PDN type (0)
✓ Protocol or Container ID: DNS Server IPv4 Address (0x000d)
  Length: 0x04 (4)
  IPv4: 8.8.8.8
✓ Protocol or Container ID: IPv4 Link MTU (0x0010)
  Length: 0x02 (2)
  IPv4 link MTU size: 1500 octets

```

| | | | | | | |
|-------|----------|-------------|-------------|------------|-----|---|
| 35... | 355.6... | 192.168.1.3 | 192.168.1.2 | S1AP/NA... | 156 | SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, ESM information response |
| 35... | 355.6... | 192.168.1.2 | 192.168.1.3 | S1AP/NA... | 264 | SACK (Ack=4, Arwnd=106496) , InitialContextSetupRequest, Attach accept, Activate def. |

```

✓ Protocol or Container ID: IPv4 Link MTU (0x0010)
  Length: 0x02 (2)
  IPv4 link MTU size: 1500 octets
✓ EPS mobile identity - GUTI
  Element ID: 0x50
  Length: 11
  .... 0... = Odd/even indication: Even number of identity digits
  .... .110 = Type of identity: GUTI (6)
  Mobile Country Code (MCC): France (208)
  Mobile Network Code (MNC): Unknown (92)
  MME Group ID: 4
  MME Code: 1
  M-TMSI: 1 (0x00000001)
✓ Item 4: id-UESecurityCapabilities
  ✓ ProtocolIE-Field
    id: id-UESecurityCapabilities (107)
    criticality: reject (0)
  ✓ value
    ✓ UESecurityCapabilities
      ✓ encryptionAlgorithms: e000 [bit length 16, 1110 0000 0000 0000 decimal value 57344]
        1... .... = 128-EEA1: Supported
        .1.. .... = 128-EEA2: Supported
        ..1. .... = 128-EEA3: Supported
        ...0 0000 0000 0000 = Reserved: 0x0000
      ✓ integrityProtectionAlgorithms: e000 [bit length 16, 1110 0000 0000 0000 decimal value 57344]
        1... .... = 128-EIA1: Supported
        .1.. .... = 128-EIA2: Supported
        ..1. .... = 128-EIA3: Supported
        .... .0. .... = EIA7: Not supported
        ...0 00.0 0000 0000 = Reserved: 0x0000
✓ Item 5: id-SecurityKey
  ✓ ProtocolIE-Field
    id: id-SecurityKey (73)
    criticality: reject (0)
  ✓ value
    SecurityKey: 3508ee9d1d95a9ca9f3d49c945e0aa8984846310e425354b8bc0dfbc08a9ea65 [bit length 256]

```


2 MARKS

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|----------|------------|-------------|----------|--------|------------------------|
| 35... | 355.6... | 127.0.11.1 | 127.0.11.2 | GTpV2 | 211 | Create Session Request |
| <div> <div> User Datagram Protocol, Src Port: 57253, Dst Port: 2123 </div> <div> <div>Source Port: 57253</div> <div>Destination Port: 2123</div> <div>Length: 175</div> <div>Checksum: 0x14c4 [unverified]</div> <div>[Checksum Status: Unverified]</div> <div>[Stream index: 175]</div> </div> <div> <div>Timestamps</div> <div> <div>[Time since first frame: 0.00000000 seconds]</div> <div>[Time since previous frame: 0.00000000 seconds]</div> </div> <div>UDP payload (167 bytes)</div> </div> </div> | | | | | | |
| <div> <div> GPRS Tunneling Protocol V2 </div> <div> <div>Flags: 0x48</div> <div> 010. = Version: 2
 ...0 = Piggybacking flag (P): 0
 1... = TEID flag (T): 1
0.. = Message Priority(MP): 0 </div> <div>Message Type: Create Session Request (32)</div> <div>Message Length: 163</div> <div>Tunnel Endpoint Identifier: 0x00000000 (0)</div> <div>Sequence Number: 0x0043d0 (17360)</div> <div>Spare: 0</div> </div> <div> <div>Recovery (Restart Counter) : 0</div> <div> <div>IE Type: Recovery (Restart Counter) (3)</div> <div>IE Length: 1</div> <div>0000 = CR flag: 0</div> <div>.... 0000 = Instance: 0</div> <div>Restart Counter: 0</div> </div> </div> <div> <div>International Mobile Subscriber Identity (IMSI) : 208920100001102</div> <div> <div>IE Type: International Mobile Subscriber Identity (IMSI) (1)</div> <div>IE Length: 8</div> <div>0000 = CR flag: 0</div> <div>.... 0000 = Instance: 0</div> <div>IMSI: 208920100001102</div> </div> <div> <div>[Association IMSI: 208920100001102]</div> <div> <div>Mobile Country Code (MCC): France (208)</div> <div>Mobile Network Code (MNC): Unknown (920)</div> </div> </div> </div> </div> | | | | | | |

- ✓ User Location Info (ULI) : TAI ECGI
 - IE Type: User Location Info (ULI) (86)
 - IE Length: 13
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - ✓ ULI Flags: 0x18, ECGI Present, TAI Present
 - 0... = Extended Macro eNodeB ID Present: False
 - .0.. = Macro eNodeB ID Present: False
 - ..0. = LAI Present: False
 - ...1 = ECGI Present: True
 - 1... = TAI Present: True
 -0.. = RAI Present: False
 -0. = SAI Present: False
 -0 = CGI Present: False
 - ✓ Tracking Area Identity (TAI)
 - Mobile Country Code (MCC): France (208)
 - Mobile Network Code (MNC): Unknown (92)
 - Tracking Area Code: 0x0001 (1)
 - ✓ E-UTRAN Cell Global Identifier (ECGI)
 - Mobile Country Code (MCC): France (208)
 - Mobile Network Code (MNC): Unknown (92)
 - Spare: 0
 - ✓ ECI (E-UTRAN Cell Identifier): 917760
 - 0000 0000 1110 0000 0001 = eNodeB Id: 3585
 - 0000 0000 = CellId: 0
- ✓ RAT Type : EUTRAN (6)
 - IE Type: RAT Type (82)
 - IE Length: 1
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - RAT Type: EUTRAN (6)
- ✓ PDN Type : IPv4
 - IE Type: PDN Type (99)
 - IE Length: 1
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - 0000 0... = Spare bit(s): 0
 -001 = PDN Type: IPv4 (1)
- ✓ PDN Address Allocation (PAA) : IPv4 0.0.0.0
 - IE Type: PDN Address Allocation (PAA) (79)
 - IE Length: 5
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 -001 = PDN Type: IPv4 (1)
 - PDN Address and Prefix(IPv4): 0.0.0.0
- ✓ APN Restriction : No Existing Contexts or Restriction (0)
 - IE Type: APN Restriction (127)
 - IE Length: 1
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - APN Restriction: No Existing Contexts or Restriction (0)
- ✓ Aggregate Maximum Bit Rate (AMBR) :
 - IE Type: Aggregate Maximum Bit Rate (AMBR) (72)
 - IE Length: 8
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - AMBR Uplink (Aggregate Maximum Bit Rate for Uplink): 50000
 - AMBR Downlink (Aggregate Maximum Bit Rate for Downlink): 100000

Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S11 MME GTP-C interface, TEID/GRE Key: 0x00000001, IPv4 127.0.0.1
IE Type: Fully Qualified Tunnel Endpoint Identifier (F-TEID) (87)
IE Length: 9
0000 = CR flag: 0
.... 0000 = Instance: 0
1... = V4: IPv4 address present
.0.. = V6: IPv6 address not present
..00 1010 = Interface Type: S11 MME GTP-C interface (10)
TEID/GRE Key: 0x00000001 (1)
F-TEID IPv4: 127.0.11.1

Access Point Name (APN) : chandhar.labs
IE Type: Access Point Name (APN) (71)
IE Length: 14
0000 = CR flag: 0
.... 0000 = Instance: 0
APN (Access Point Name): chandhar.labs

Selection Mode : MS or network provided APN, subscribed verified
IE Type: Selection Mode (128)
IE Length: 1
0000 = CR flag: 0
.... 0000 = Instance: 0
.... ..00 = Selection Mode: MS or network provided APN, subscribed verified (0)

Serving Network : MCC 208 France, MNC 92
IE Type: Serving Network (83)
IE Length: 3
0000 = CR flag: 0
.... 0000 = Instance: 0
Mobile Country Code (MCC): France (208)
Mobile Network Code (MNC): Unknown (92)

Bearer Context : [Grouped IE]
IE Type: Bearer Context (93)
IE Length: 31
0000 = CR flag: 0
.... 0000 = Instance: 0

5. In Wireshark view the message details of UE Capability Info Indication and Information communicated via slap protocol.

NOTE: At Step 5, take a screenshot and attach it.

Highlight the initial message fields

2 MARKS

The screenshot shows the Wireshark interface with the S1AP protocol selected. The packet list displays a packet from 192.168.1.3 to 192.168.1.2, identified as S1AP, with a length of 192 bytes. The packet details pane shows the structure of the initiatingMessage, including procedureCode (id-UECapabilityInfoIndication (22)), criticality (ignore (1)), and value. The value field is expanded to show UE Capability Info Indication details, including protocolIEs (id-MME-UE-S1AP-ID, id-eNB-UE-S1AP-ID, id-UERadioCapability) and their respective fields and values. The id-MME-UE-S1AP-ID field is highlighted with a yellow box, showing the value 1. The id-eNB-UE-S1AP-ID field is also highlighted with a yellow box, showing the value 12041263.

```

    No.  Time  Source      Destination  Protocol  Length  Info
    ---  ---  ---
    35... 355.7... 192.168.1.3  192.168.1.2  S1AP      192      UECapabilityInfoIndication, UECapabilityInformation

    Details:
    +---+
    | initiatingMessage |
    +---+
    | procedureCode: id-UECapabilityInfoIndication (22) |
    | criticality: ignore (1) |
    | value |
    +---+
    | UE Capability Info Indication |
    +---+
    | protocolIEs: 3 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: 12041263 |
    +---+
    | Item 2: id-UERadioCapability |
    +---+
    | ProtocolIE-Field |
    +---+
    | id: id-UERadioCapability (74) |
    | criticality: reject (0) |
    | value |
    +---+
    | UERadioCapability [truncated]: 042fc801085f5ddb80512193820e002010644913326d0a54ca14 |
    +---+
    | UERadioAccessCapabilityInformation |
    +---+
    | criticalExtensions: c1 (0) |
    +---+
    | c1: ueRadioAccessCapabilityInformation-r8 (0) |
    +---+
    | ueRadioAccessCapabilityInformation-r8 |
    +---+
    | ue-RadioAccessCapabilityInfo [truncated]: 00210bebbb700a24327041c0 |
    +---+
    | UECapabilityInformation |
    +---+
    | rrc-TransactionIdentifier: 0 |
    | criticalExtensions: c1 (0) |
    +---+
    | c1: ueCapabilityInformation-r8 (0) |
    +---+
    | ueCapabilityInformation-r8 |
    +---+
    | ue-CapabilityRAT-ContainerList: 1 item |
    +---+
    | Item 0 |
    +---+
    | UE-CapabilityRAT-Container |
    +---+
    | rat-Type: eutra (0) |
    | ueCapabilityRAT-Container [truncated]: c |
    +---+
    | UE-EUTRA-Capability |
    +---+
  
```

6. In Wireshark view the message details of Initial Context Setup Response, Attach complete and the activation of default EPS bearer context accept communicated via s1ap protocol.

*NOTE: At Step 6, take a screenshot and attach it.
Highlight the initial message fields*

The screenshot shows the Wireshark interface with the 's1ap' protocol selected. The packet list shows a packet of length 264, identified as 'SACK (Ack=4, Arwnd=106496), InitialContextSetupRequest, Attach a...'. The packet details pane is expanded to show the 'value' field of the 'UEAggregateMaximumBitrate' field, which contains the following information:

- id-MME-UE-S1AP-ID (0)
- id-eNB-UE-S1AP-ID (8)
- id-E-RABToBeSetupListCtxtSUReq (24)
- id-UESecurityCapabilities (107)
- id-SecurityKey (73)
- UEAggregateMaximumBitrateDL: 1000000000bits/s
- UEAggregateMaximumBitrateUL: 500000000bits/s

The 'SecurityKey' field is also highlighted, showing the value '3508ee9d1d95a9ca9f3d49c945e0aa8984846310e425354b8bc0dfbc08a9ea65' with a bit length of 256.

INFERENCE & ANALYSIS

From the above inlab, illustrate the 4G LTE cellular system IP allocation sequence. Map the modules using a pictorial illustration.

