

Physical Channels: Handled by the Physical Layer (PHY), directly dealing with radio signal transmission and reception. Ensure that the signals are properly transmitted over the air and are received with the correct timing and frequency.

Transport Channels: Managed by the Medium Access Control (MAC) layer. Map logical channels to physical channels and manage the transport of data and control information. Ensure that data and control information from logical channels are correctly transported using physical channels.

Logical Channels: Defined at higher layers such as RLC, PDCP, and SDAP. They categorize the type of information being exchanged. Organize the information into different types (broadcast, control, or dedicated) and specify how it should be transmitted over the transport channels.

In summary, Physical channels deal with the actual radio transmission, transport channels handle the mapping of data to physical channels, and logical channels define the type of information being communicated.

Physical Channels

- **Physical Channels:** These are the actual radio signals transmitted over the air. They correspond to physical layer operations.
 - **PSS (Primary Synchronization Signal):** A physical signal used for cell search and initial synchronization.
 - **SSS (Secondary Synchronization Signal):** A physical signal that helps the UE achieve frequency synchronization and cell identification.
 - **PRACH (Physical Random Access Channel):** A physical channel used by the UE to initiate random access procedures.
 - **PUSCH (Physical Uplink Shared Channel):** Used for uplink data transmission from the UE to the gNB.
 - **PDSCH (Physical Downlink Shared Channel):** Used for downlink data transmission from the gNB to the UE.

2. Transport Channels

- **Transport Channels:** These channels map the logical channels to physical channels and handle the transport of data and control information.
 - **UCI (Uplink Control Information):** Includes **HARQ (Hybrid Automatic Repeat reQuest)** ACK/NACK, **CQI (Channel Quality Indicator)**, and **Scheduling Request**, carried on the **PUSCH**.
 - **DL-SCH (Downlink Shared Channel):** Carries user data and control information from the gNB to the UE, mapped onto the **PDSCH**.
 - **UL-SCH (Uplink Shared Channel):** Carries user data from the UE to the gNB, mapped onto the **PUSCH**.

3. Logical Channels

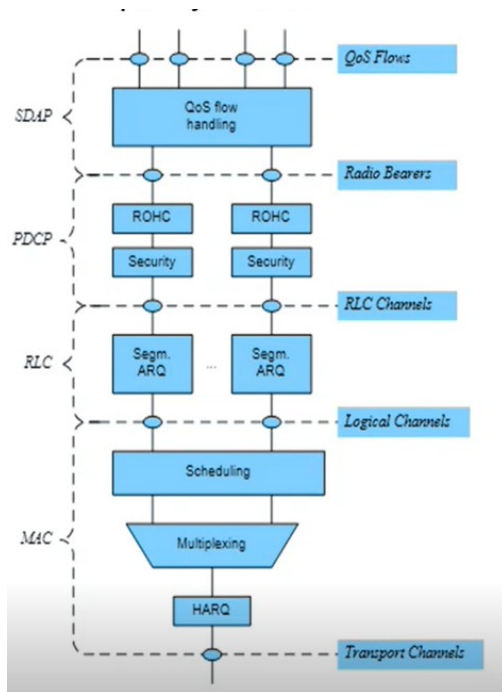
- **Logical Channels:** These are the channels defined in the higher layers of the protocol stack and specify the type of information being exchanged.
 - **BCCH (Broadcast Control Channel):** Used to broadcast system information (e.g., MIB, SIBs) from the gNB to the UE. It is mapped onto the **PDSCH**.
 - **CCCH (Common Control Channel):** Used for sending control information for connection establishment and management. It is carried by the **DL-SCH**.
 - **DCCH (Dedicated Control Channel):** Used for dedicated control messages between the UE and gNB. It is mapped onto the **DL-SCH** for downlink and **UL-SCH** for uplink.
 - **DSCH (Dedicated Shared Channel):** Carries user data and signaling on a dedicated basis. It is mapped onto the **PDSCH** for downlink and **PUSCH** for uplink.
-

📡 **Shared Channels:** Called "Shared" because they are used for data and control information applicable to multiple UEs.

📡 **Control Channels:** Named "Control" due to their role in carrying signaling and control information for managing connections.


📡 **Synchronization Channels:** Called "Synchronization" because they help synchronize the UE with the network.

📡 **Random Access Channels:** Named for their function in initiating access requests randomly.



📡 **RRC_IDLE:** Indicates that the RRC layer is not actively connected to the gNB. The UE can receive broadcast information and perform cell search but does not have an active connection.

📡 **RRC_INACTIVE:** Indicates that the RRC layer has an existing but reduced connection with the gNB. It balances resource usage and power savings while keeping PDU sessions active.

 **RRC_CONNECTED:** Indicates that the RRC layer has an active and fully established connection with the gNB, allowing full data and control communication.

DETAILED STEPS:

1. UE Power On

- The **UE** powers on and starts scanning for available 5G cells.
- It searches for the appropriate frequency bands to connect to the network.

2. Cell Search/ Downlink Synchronization

- The **UE** performs a cell search to detect the **PSS** and **SSS** transmitted by the **gNB**.
- These signals help the **UE** to identify the cell and synchronize its timing with the **gNB**.
- **PSS (Primary Synchronization Signal):** A physical signal used for cell search and initial synchronization.
- **SSS (Secondary Synchronization Signal):** A physical signal that helps the UE achieve frequency synchronization and cell identification.

3. Cell Search and Synchronization

- The **UE** continues the synchronization process by decoding the **PBCH** to obtain the **Master Information Block (MIB)**, which contains essential information for initial network access, including system timing, system frame Number, and cell identity. This information is necessary for the **UE** to initiate network access and proceed with further communication steps.
- The **PBCH** carries vital system information (MIB) that helps the UE synchronize with the network and connect properly.

```
message {  
  Mib {  
    systemFrameNumber = { 6, 000000xx }  
    subCarrierSpacingCommon = scs30or120  
    ssb_SubcarrierOffset = 0  
    dmrs_TypeA_Position = pos3  
    pdccch_ConfigSIB1 {  
      controlResourceSetZero = 10  
      searchSpaceZero = 0  
    }  
    cellBarred = notBarred  
    intraFreqReselection = allowed  
    spare = { 1, 0xxxxxxx }  
  }  
}
```

4. System Information Acquisition

- The **UE** reads **System Information Blocks (SIBs)**, particularly **SIB1**, which provides crucial information like the **PLMN ID (Public Land Mobile Network Identifier)** and identity.

```

819         ci {
820             SystemInformationBlockType1 {
821                 cellSelectionInfo {
822                     q_RxLevMin = -70
823                     q_RxLevMinOffset = 1
824                     q_QualMin = -12
825                     q_QualMinOffset = 1
826                 }
827                 cellAccessRelatedInfo {
828                     plmn_IdentityInfoList[0] {
829                         plmn_IdentityInfoList[0] {

```

This PLMN ID is also stored in SIM in MOBILE. If this matches with the sib then it will camp on to the cell.

5. Uplink Synchronization

- The **UE** initiates the uplink synchronization using the **RACH** process.
- The **UE** transmits a randomly chosen preamble to the **gNB**. (MSG 1)
- The **gNB** detects the preamble and responds with a Random Access Response (RAR), which includes Timing Advance, Temporary C-RNTI (Cell Radio Network Temporary Identifier), and an Uplink Grant, this enables the **UE** to align its uplink transmission timing with the **gNB**. (MSG 2)

The total number of preambles available for the Random Access Channel (RACH) is **64**.

6. RRC Connection Establishment / Random Access Procedure

- The **UE** sends an **RRC Connection Request** on **PUSCH ((MSG 3 (UE Scheduled Transmission)))**, which is then responded to by the **gNB** with an **RRC Connection Setup** on **PDSCH. (MSG 4 (Contention Resolution))**
- The **UE** confirms this with an **RRC Connection Setup Complete** message. And with this



we also send NAS Registration to the gNB

7. Registration Request (NG Interface)

- The **UE** sends a **Registration Request** message to the **gNB**, which forwards it to the **AMF (Access and Mobility Management Function)** over the **NG-C (Next Generation Control)** interface using **NGAP (Next Generation Application Protocol)**.

This message contains important information about the **UE's** identity, security credentials, and network capabilities, and this is necessary for **UE's** attempt to register with the 5G network.

- The **AMF** processes the request, checks the **UE's** identity, subscription, and location information, and then sends a **Registration Accept** message back to the **UE** through the **gNB**.

8. Authentication and Security (NG Interface)

- The **AMF** initiates an **Authentication Request**, which is forwarded to the **UE** through the **gNB**.
- The **UE** computes and responds with an **Authentication Response**.
- The **AMF** sends a **Security Mode Command** to establish security keys and algorithms, which the **UE** acknowledges with a **Security Mode Complete** message.

This command specifies the security algorithms to be used for encrypting and protecting the integrity of the data exchanged between the UE and the network.

- **9. UE Capability Enquiry and AS Security Mode Command :**
gNB enquire the UE capability by sending UE capability enquiry Request. After that gNB will receive back UE capability Information, then gNB will update these capability to AMF.

This request asks the UE to report its supported radio capabilities (e.g., supported frequency bands, LTE/NR features, etc.). This message contains details about the UE's radio capabilities, helping the network optimize bearer setup and other configurations.

The gNB sends a Security Mode Command message to the UE to notify the UE to start the integrity protection and encryption process.

Ensures that the data exchanged over the air interface is encrypted and integrity protected. Integrity protection helps keep the communication safe by ensuring the messages are exactly as they were sent and haven't been messed with.

Then, UE derives the key according to the integrity protection and encryption algorithm indicated by the Security Mode Command message, and then replies the Security Mode Complete message to the gNB.

- **SRB2 and DRB establishment:** The gNB issues an RRC Reconfiguration message to the UE to establish SRB2 and DRB. After SRB2 and DRB are successfully established, the UE replies to the gNB with an RRC Reconfiguration Complete message. The gNB signals the successful setup DRB with **INITIAL CONTEXT SETUP RESPONSE** message to the AMF.
- **Registration Complete and PDU session Establishment:** UE send Registration Complete and PDU session establishment request to AMF

9. PDU Session Establishment (NG Interface)

The UE can now establish a PDU (Packet Data Unit) session with the 5G Core Network. This session allows the UE to exchange data with the network.

- The **UE** requests a **PDU Session Establishment** via the **gNB** to the **AMF**, which then forwards it to the **SMF (Session Management Function)**.
- The **SMF** processes the request and sends a **PDU Session Establishment Accept** back to the **UE** via the **AMF** and **gNB**.
- The **gNB** configures the necessary radio bearers for the **PDU session** with an **RRC Reconfiguration** message.
- The **UE** confirms this with an **RRC Reconfiguration Complete** message.

The RRC Reconfiguration lays the groundwork for the PDU session by establishing the necessary radio bearers, and the PDU session establishment configures the data path through these bearers, enabling actual user data transmission.(for modification in the RRC connection)

This is SRB 2 , bcz the SRB1 is default which is used for the signaling purposes. And this DRB is created here only bcz it is used for carrying data.

- A **Radio Bearer** in 5G is a service that transfers data between the UE and gNB, with SRBs for control signaling and DRBs for user data, ensuring proper QoS (Quality of Service) by meeting specific requirements like data rate, latency, and reliability, and managing resources effectively.
- **Quality of Service (QoS)** in 5G refers to the performance level of a service, ensuring specific requirements like data rate, latency, and reliability are met for different types of traffic (e.g., voice, video). QoS guarantees that critical applications receive the necessary resources for optimal performance.
- **QoS (Quality of Service)** in 5G sets the priority for different types of traffic. It ensures that high-priority applications, like voice or critical data, receive the necessary resources and performance levels (e.g., lower latency and higher data rates) compared to lower-priority traffic. This prioritization helps maintain the quality and efficiency of network services.

10. Attach Complete

11. Data Transfer (NG Interface)

- Data is transferred between the **UE** and the 5G Core network through the **gNB** via the **NG-U (Next Generation User)** interface.
- The **gNB** forwards the user data to the **UPF (User Plane Function)**.

Bearers are created for transferring user data. These bearers are mapped to different QoS (Quality of Service) levels depending on the type of data.

Handover and Mobility

- If the UE moves out of the coverage area of the current gNB, a handover procedure will be initiated to transfer the connection to another gNB.