Cell Search and Downlink Synchronization: Cell search is the procedure by which a UE acquires time and frequency synchronization with a cell, decode the Cell ID and PBCH (MIB) information. Detailed procedure can be read in this post.

Uplink Synchronization:

UE can achieve UL synchronization can by RACH Procedure. All RACH access related parameters UE can retrieve from System Information#1.  For RACH procedure, UE select a random preamble (msg#1), this preamble is referenced with the RAP ID. UE also starts a timing T300 to await the RRC Setup message from the gNB.

gNB detect the RACH Msg#1 and send a DCI Format 1\_0 with CRC scrambled by a the RA-RNTI corresponding to the RACH transmission. This DCI contains Frequency  and Time resource assignment, and MCS for Msg#2 RAR sent on PDSCH.

UE tries to DCI Format 1\_0 with CRC scrambled by the corresponding RA-RNTI and MAC transport block in a corresponding PDSCH having RAR Msg#2 information including timing advance, uplink grant and the Temporary C-RNTI assignment.

RRC Connection Request: RRC Connection request is considered as Msg#3 and it includes ue-Identity, establishment Cause. The ue-identity can be a Random number between 0 and 2^39-1 and will be used to contention resolution by UE while decoding Msg#4 RRC connection setup. RRC Connection Request is sent on the UL grant provides in Msg#2 from the gNB and over SRB0 on UL common control Channel(UL\_CCCH).

Apply below things for msg#3

> apply the default L1 parameter values as specified in corresponding physical layer specifications except for the parameters for which values are provided in SIB1; 1> apply the default MAC Cell Group configuration as specified in 9.2.2; 1> apply the CCCH configuration as specified in 9.1.1.2; 1> apply the timeAlignmentTimerCommon included in SIB1; 1> start timer T300; 1> initiate transmission of the RRCSetupRequest message in accordance with 5.3.3.3;

RRC setup: The RRC Setup message is sent to setup SRB1, contention resolution and the master cell configuration. The UE stops the timer T300 as it has received the RRC Setup message. It carries following information elements.

radioBearerConfig {srb-ToAddModList},

masterCellGroup { cellGroupId,  rlc-BearerToAddModList, mac-CellGroupConfig, physicalCellGroupConfig}

Reception of the RRCSetup by the UE The UE shall perform the following actions upon reception of the RRCSetup:

1> perform the cell group configuration procedure in accordance with the received masterCellGroup and as specified in 5.3.5.5; 1> perform the radio bearer configuration procedure in accordance with the received radioBearerConfig and as specified in 5.3.5.6; 1> if stored, discard the cell reselection priority information provided by the cellReselectionPriorities or inherited from another RAT; 1> stop timer T300, T301 or T319 if running; 1> if T390 is running: 2> stop timer T390 for all access categories; 2> perform the actions as specified in 5.3.14.4; 1> if T302 is running: 2> stop timer T302; 2> perform the actions as specified in 5.3.14.4; 1> stop timer T320, if running; 1> if the RRCSetup is received in response to an RRCResumeRequest, RRCResumeRequest1 or RRCSetupRequest: 2> if T331 is running: 3> stop timer T331; 3> perform the actions as specified in 5.7.8.3; 2> enter RRC\_CONNECTED; 2> stop the cell re-selection procedure; 1> consider the current cell to be the PCell; 1> set the content of RRCSetupComplete message as follows: 2> if upper layers provide a 5G-S-TMSI: 3> if the RRCSetup is received in response to an RRCSetupRequest: 4> set the ng-5G-S-TMSI-Value to ng-5G-S-TMSI-Part2; 3> else: 4> set the ng-5G-S-TMSI-Value to ng-5G-S-TMSI; 2> if upper layers selected an SNPN or a PLMN and in case of PLMN UE is either allowed or instructed to access the PLMN via a cell for which at least one CAG ID is broadcast: 3> set the selectedPLMN-Identity from the npn-IdentityInfoList; 2> else: 3> set the selectedPLMN-Identity to the PLMN selected by upper layers from the plmn-IdentityList; 2> if upper layers provide the 'Registered AMF': 3> include and set the registeredAMF as follows: 4> if the PLMN identity of the 'Registered AMF' is different from the PLMN selected by the upper layers: 5> include the plmnIdentity in the registeredAMF and set it to the value of the PLMN identity in the 'Registered AMF' received from upper layers; 4> set the amf-Identifier to the value received from upper layers; 3> include and set the guami-Type to the value provided by the upper layers; 2> if upper layers provide one or more S-NSSAI (see TS 23.003 [21]): 3> include the s-NSSAI-List and set the content to the values provided by the upper layers; 2> set the dedicatedNAS-Message to include the information received from upper layers; 2> if connecting as an IAB-node: 3> include the iab-NodeIndication; 2> if the SIB1 contains idleModeMeasurementsNR and the UE has NR idle/inactive measurement information concerning cells other than the PCell available in VarMeasIdleReport; or 2> if the SIB1 contains idleModeMeasurementsEUTRA and the UE has E-UTRA idle/inactive measurement information available in VarMeasIdleReport: 3> include the idleMeasAvailable; 2> if the UE has logged measurements available for NR and if the RPLMN is included in plmn-IdentityList stored in VarLogMeasReport: 3> include the logMeasAvailable in the RRCSetupComplete message; 3> if Bluetooth measurement results are included in the logged measurements the UE has available for NR and if the RPLMN is included in plmn-IdentityList stored in VarLogMeasReport: 4> include the logMeasAvailableBT in the RRCSetupComplete message; ETSI 3GPP TS 38.331 version 16.4.1 Release 16 58 ETSI TS 138 331 V16.4.1 (2021-04) 3> if WLAN measurement results are included in the logged measurements the UE has available for NR and if the RPLMN is included in plmn-IdentityList stored in VarLogMeasReport: 4> include the logMeasAvailableWLAN in the RRCSetupComplete message; 2> if the UE has connection establishment failure or connection resume failure information available in VarConnEstFailReport and if the RPLMN is equal to plmn-Identity stored in VarConnEstFailReport: 3> include connEstFailInfoAvailable in the RRCSetupComplete message; 2> if the UE has radio link failure or handover failure information available in VarRLF-Report and if the RPLMN is included in plmn-IdentityList stored in VarRLF-Report, or 2> if the UE has radio link failure or handover failure information available in VarRLF-Report of TS 36.331 [10], and if the UE is capable of cross-RAT RLF reporting and if the RPLMN is included in plmnIdentityList stored in VarRLF-Report of TS 36.331 [10]: 3> include rlf-InfoAvailable in the RRCSetupComplete message; 2> if the UE supports storage of mobility history information and the UE has mobility history information available in VarMobilityHistoryReport: 3> include the mobilityHistoryAvail in the RRCSetupComplete message; 2> if the RRCSetup is received in response to an RRCResumeRequest, RRCResumeRequest1 or RRCSetupRequest: 3> if speedStateReselectionPars is configured in the SIB2: 4> include the mobilityState in the RRCSetupComplete message and set it to the mobility state (as specified in TS 38.304 [20]) of the UE just prior to entering RRC\_CONNECTED state; 1> submit the RRCSetupComplete message to lower layers for transmission, upon which the procedure ends.

RRC setup Complete + Registration Request: The UE sends the RRC Setup Complete message with a “Registration Request” in the dedicatedNAS-Message. It also carries the information about selectedPLMN-Identity, registeredAMF, snssai-list. Registration request also carries UE network capability information. The gNB selects the Access and Mobility Function (AMF) for this session and allocate RAN UE NGAP ID to the UE. The AMF will use this id to address the UE context on the gNB.

Initial UE Message: The gNB sends the Initial UE Message to the selected AMF. The message carries the “Registration Request” message received from the UE in the RRC Setup Complete message. The “RAN UE NGAP ID” and the “RRC Establishment Cause” are also included in the message.

the transmission of NAS security related parameters encapsulated in the AS signalling from the AMF to the UE triggering the inter-system change in 5GMM-CONNECTED mode (see 3GPP TS 33.501 [24]). The UE uses these parameters to generate the mapped 5G NAS security context (see subclause 8.6.2 of 3GPP TS 33.501 [24]); and

after the inter-system change in 5GMM-CONNECTED mode, the transmission of a REGISTRATION REQUEST message from the UE to the AMF. The UE shall send this message integrity protected using the mapped 5G NAS security context and further protect this message as specified in subclause 4.4.6 and subclause 5.5.1.3.2. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected using the mapped 5G NAS security context, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered using the mapped 5G NAS security context.

a) if the UE has a valid native 5G NAS security context, the UE shall transmit a REGISTRATION REQUEST message integrity protected with the native 5G NAS security context. The UE shall include the ngKSI indicating the native 5G NAS security context value in the REGISTRATION REQUEST message. After receiving the REGISTRATION REQUEST message including the ngKSI indicating a native 5G NAS security context value, the AMF shall check whether the ngKSI included in the REGISTRATION REQUEST message belongs to a 5G NAS security context available in the AMF, and shall verify the MAC of the REGISTRATION REQUEST message. If the verification is successful, the AMF deletes the EPS security context received from the source MME if any, and the AMF re-establishes the secure exchange of NAS messages by either:

1) replying with a REGISTRATION ACCEPT message that is integrity protected and ciphered using the native 5G NAS security context. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered; or 2) initiating a security mode control procedure. This can be used by the AMF to take a non-current 5G NAS security context into use or to modify the current 5G NAS security context by selecting new NAS security algorithms.

Authentication and NAS Security: The Core network performs Authentication procedure for the UE is legitimate and legally authorized to get service from the network. The detailed authentication procedure can be read from this post. The AMF signals the selected NAS security algorithm to the UE and requests the IMEISV from the UE as part of NAS security mode command. UE respond with completion of the NAS security procedure and contains the IMEISV in security mode complete.

AS UE Capability Transfer and AS Security: gNB can enquire the UE capability with UE capability enquiry and Information. After receiving from UE capability gNB update these capability to AMF.  The gNB sends a Security Mode Command message to the UE to notify the UE to start the integrity protection and encryption process. After that, downstream encryption is started. The 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. After that, the upstream encryption is started.;l

The network initiates the procedure to a UE in RRC\_CONNECTED when it needs (additional) UE radio access capability information. The network should retrieve UE capabilities only after AS security activation. Network does not forward UE capabilities that were retrieved before AS security activation to the CN.

SRB2 and DRB establishment: The gNB issues an RRC Reconfiguration message to the UE to establish SRB2 and DRB. After the 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

The purpose of this procedure is to modify an RRC connection, e.g. to establish/modify/release RBs, to perform reconfiguration with sync, to setup/modify/release measurements, to add/modify/release SCells and cell groups, to add/modify/release conditional handover configuration, to add/modify/release conditional PSCell change configuration. As part of the procedure, NAS dedicated information may be transferred from the Network to the UE.

5.3.5.2 Initiation The Network may initiate the RRC reconfiguration procedure to a UE in RRC\_CONNECTED. The Network applies the procedure as follows: - the establishment of RBs (other than SRB1, that is established during RRC connection establishment) is performed only when AS security has been activated; - the addition of Secondary Cell Group and SCells is performed only when AS security has been activated; - the reconfigurationWithSync is included in secondaryCellGroup only when at least one RLC bearer is setup in SCG; - the reconfigurationWithSync is included in masterCellGroup only when AS security has been activated, and SRB2 with at least one DRB or, for IAB, SRB2, are setup and not suspended; - the conditionalReconfiguration for CPC is included only when at least one RLC bearer is setup in SCG; - the conditionalReconfiguration for CHO is included only when AS security has been activated, and SRB2 with at least one DRB or, for IAB, SRB2, are setup and not suspended.

Registration Complete and PDU session Establishment: UE send Registration Complete and PDU session establishment request to AMF. PDU session establishment is similar to PDN Connectivity Request message in LTE. AMF sends a PDU SESSION RESOURCE SETUP REQUEST message to gNB carrying the list of PDU sessions that need to be established, the list of QoS Flows for each PDU session, and the quality attributes of each QoSFlow. The gNB maps the QoS Flow to the QoS Flow according to the quality attributes of the QoS Flow. gNB  send NAS PDU session establishment accept.