

# Verizon 5G TF; Network and Signaling Working Group; Verizon 5th Generation Radio Access; Overall Description (Release 1)

June 29, 2016

Cisco, Ericsson, Intel Corp., LG Electronics, Nokia, Samsung Electronics, Qualcomm Technologies Inc.

V1.0

V 1.0

**Disclaimer:** This document provides information related to 5G technology. All information provided herein is subject to change without notice. The members of the 5GTF disclaim and make no guaranty or warranty, express or implied, as to the accuracy or completeness of any information contained or referenced herein. THE 5GTF AND ITS MEMBERS DISCLAIM ANY IMPLIED WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE, AND ALL INFORMATION IS PROVIDED ON AN "AS-IS" BASIS. No licenses under any intellectual property of any kind are provided by any person (whether a member of the 5GTF or not) that may be necessary to access or utilize any of the information contained herein, including, but not limited to, any source materials referenced herein, and any patents required to implement or develop any technology described herein. It shall be the responsibility of anyone attempting to use the information contained or referenced herein to obtain any such licenses, if necessary. The 5GTF and its members disclaim liability for any damages or losses of any nature whatsoever whether direct, indirect, special or consequential resulting from the use of or reliance on any information contained or referenced herein.

© 2016 Cellco Partnership d/b/a Verizon Wireless; All rights reserved

## Document History

---

Version	Date	Change	Verizon POC
0.0.1	2016-03-04	Draft version created	
0.0.2	2016-03-11	Updated based on initial review in workstream	
0.0.3	2016-03-16	Updated based on email comments	
0.0.7	2016-04-08	Updated based on conference call 5	
0.1.0	2016-04-28	Updated based on F2F meeting 4	
1.0	2016-06-29	Approved version	

## Document Approvals

---

Name	Title	Company	Date of Approval

## Table of Contents

---

### Scope

#### 2 References

#### 3 Definitions and abbreviations

- 3.1 Definitions
- 3.2 Abbreviations

#### 4 Overall architecture

- 4.1 Architecture principles
- 4.2 Radio protocol architecture
  - 4.3.1 User plane
  - 4.3.2 Control plane
- 4.3 Radio access network identities

#### 5 RAN-UE signalling: 5G-RRC

- 5.1 Services and Functions
- 5.2 RRC protocol states & state transitions
- 5.3 Transport of NAS messages
- 5.4 System Information
- 5.5 RRC Connection Setup

#### 6 RAN-CN signalling and user plane: NG1-C and NG1-U

#### 7 5G L2 user plane

- 7.1 5G Medium Access Control
  - 7.1.1 Services and Functions
  - 7.1.2 Logical Channels
  - 7.1.3 Mapping between logical channels and transport channels
  - 7.1.4 PDU Structure
- 7.2 5G Radio Link Control
  - 7.2.1 Services and Functions
  - 7.2.2 PDU Structure
- 7.3 5G Packet Data Convergence Protocol
  - 7.3.1 Services and Functions
  - 7.3.2 PDU Structure

#### 8 Mobility

- 8.1 Intra 5G-RAN
- 8.2 Radio Link Failure

8.3 Measurements

## **9 ARQ**

## **10 Scheduling**

10.1 Basic Scheduler Operation

10.2 Measurements to Support Scheduler Operation

## **11 Carrier Aggregation**

11.1 Principles

11.2 Layer 2 Structure

## **14 Security**

14.1 Overview and Principles

14.2 Security termination points

14.3 State Transitions and Mobility

14.3.1 RRC\_IDLE to RRC\_CONNECTED

14.3.2 RRC\_CONNECTED to RRC\_IDLE

14.3.3 Intra 5G RAN Mobility

14.4 AS Key Change in RRC\_CONNECTED



## 1 Scope

---

The present document provides an overview and overall description of the radio network and protocol architecture of the Verizon 5G system for initial Fixed Wireless Use case.

## 2 References

---

- [1] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture".

## 3 Definitions and abbreviations

---

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

**5G-RRC:** the protocol used for signaling between Verizon 5G radio network and a UE.

**NG1-C:** the protocol used for signaling between Verizon 5G radio and core network control plane network function.

**Cell:** combination of downlink and uplink resources

### 3.2 Abbreviations

5G-NB	5G Node B
5G-RA	5G Radio Access
5G-RAN	5G Radio Access Network
AM	Acknowledged Mode
ARQ	Automatic Repeat Request
HARQ	Hybrid ARQ
MAC	Medium Access Control
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
RLC	Radio Link Control
RRC	Radio Resource Control
SDU	Service Data Unit
TM	Transparent Mode
UM	Unacknowledged Mode
xBCH	5G Broadcast Channel
xBCCH	5G Broadcast Control Channel
xCCCH	5G Common Control Channel
xDCCH	5G Dedicated Control Channel
xDL-SCH	5G Downlink Shared Channel
xDTCH	5G Dedicated Traffic Channel
xRACH	5G Random Access Channel
xUL-SCH	5G Uplink Shared Channel

## 4 Overall architecture

---

Editor’s note: Overall system architecture will be specified in V5G.401

Editor’s note: The workstream will initially focus on 5G fixed wireless use case but assures forward compatibility for other use cases

The 5G-RAN consists of 5GNBs, providing the 5G-RAN user plane (PDCP/RLC/MAC/PHY) and control plane (RRC) protocol terminations towards the UE. The 5GNB are connected by means of the 5G1 interface to the NG core network.

The 5G-RAN architecture is illustrated in Figure 4-1 below.

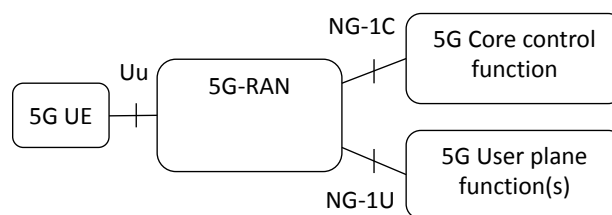


Figure 4-1: Overall Architecture

### 4.1 Architecture principles

See V5G.401.

### 4.2 Radio protocol architecture

In this subclause, the radio protocol architecture of 5G-RAN is given for the user plane and the control plane.

#### 4.3.1 User plane

The figure below shows the protocol stack for the user-plane, where PDCP, RLC and MAC sublayers (terminated in 5G-NB on the network side) perform the functions listed for the user plane in subclause 7, e.g. ciphering, scheduling, ARQ and HARQ.

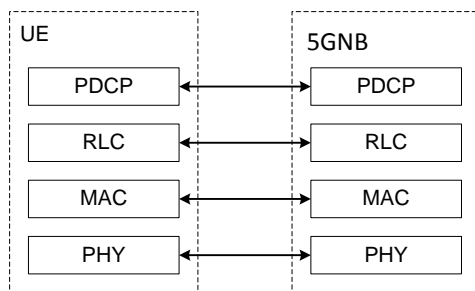


Figure 4.3.1-1: User-plane protocol stack

### 4.3.2 Control plane

The figure below shows the protocol stack for the control-plane, where:

- PDCP sublayer (terminated in 5GNB on the network side) performs the functions listed for the control plane in subclause 7, e.g. ciphering and integrity protection;
- RLC and MAC sublayers (terminated in 5GNB on the network side) perform the same functions as for the user plane;
- RRC (terminated in 5GNB on the network side) performs the functions listed in subclause 5;
- NAS control protocol (terminated in NG Core control function on the network side) performs among other things:
  - EPS bearer management;
  - Authentication;
  - Security control.

NOTE: The NAS control protocol is not covered by the scope of this TS and is only mentioned for information.

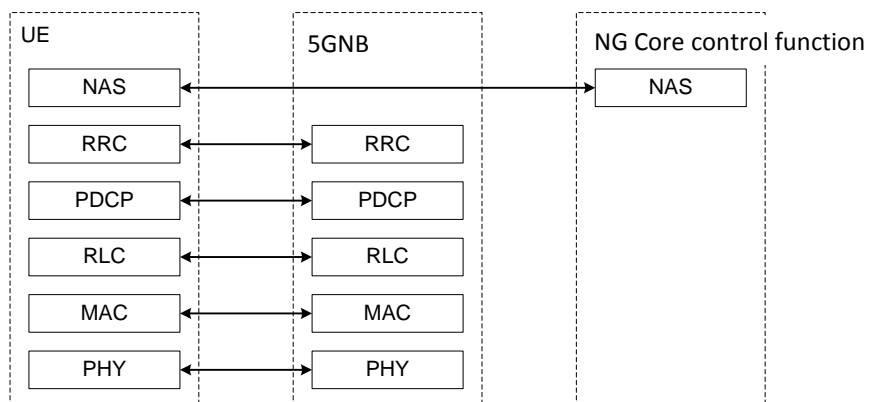


Figure 4.3.2-1: Control-plane protocol stack

### 4.3 Radio access network identities

The following 5G-RAN related UE identities are used at cell level:

- C-RNTI: unique identification used for identifying RRC Connection and scheduling;
- Temporary C-RNTI: identification used for the random access procedure;
- Random value for contention resolution: during some transient states, the UE is temporarily identified with a random value used for contention resolution purposes.

## 5 RAN-UE signalling: 5G-RRC

---

Editor's note: Device expected to be in RRC-CONNECTED. Idle mode needed for cell selection only.

This subclause provides an overview on services and functions provided by the 5G-RRC sublayer.

### 5.1 Services and Functions

The main services and functions of the RRC sublayer include:

- Broadcast of System Information related to the non-access stratum (NAS);
- Broadcast of System Information related to the access stratum (AS);
- Establishment, maintenance and release of an 5G-RRC connection:
  - Allocation of temporary identifiers between UE and E-UTRAN;
  - Configuration of signalling radio bearer(s) for RRC connection;
- Security functions including key management;
- Establishment, configuration, maintenance and release of point to point Radio Bearers;
- Mobility functions including 5G cell addition/release, UE measurement reporting, control of the reporting and UE based mobility;
- NAS direct message transfer to/from NAS from/to UE.

### 5.2 RRC protocol states & state transitions

RRC uses the following states:

- **RRC\_IDLE:**
  - PLMN selection;
  - Broadcast of system information;
  - Cell selection mobility;



- **RRC\_CONNECTED:**
  - UE has a 5G-RRC connection;
  - UE has context in 5G-RAN;
  - Network can transmit and/or receive data to/from UE;
  - At PDCP/RLC/MAC level:
    - UE can transmit and/or receive data to/from network;
    - UE monitors control signalling channel for shared data channel to see if any transmission over the shared data channel has been allocated to the UE;
    - UE also reports channel quality information and feedback information to 5G-NB;

### 5.3 Transport of NAS messages

The AS provides reliable in-sequence delivery of NAS messages in a cell. During mobility, message loss or duplication of NAS messages can occur.

NOTE: NAS messages are integrity protected and ciphered by PDCP, in addition to the integrity protection and ciphering performed by NAS.

### 5.4 System Information

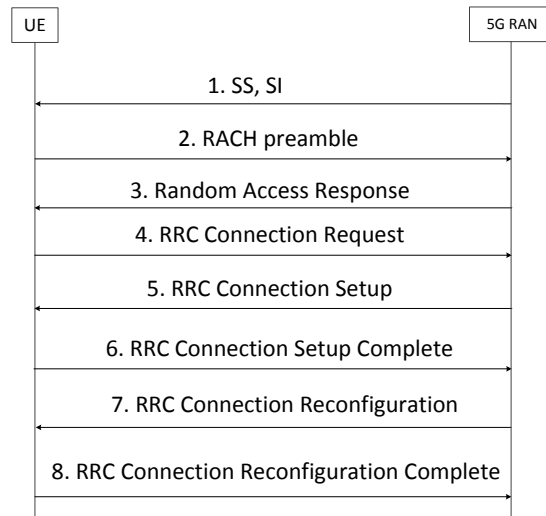
System information is divided into the *MasterInformationBlock* (MIB) and the *xSystemInformationBlocks* (xSIB):

- *MasterInformationBlock* defines the most essential physical layer information of the cell required to receive further system information;
- *SystemInformationBlock* defines the information needed to access the system.

All other information is transmitted using dedicated messages.

### 5.5 RRC Connection Setup

5G-RRC Setup procedure is initiated when 5G-RRC connection is required. Figure 5.5-1 shows 5G-RRC setup procedure.



**Figure 5.5-1 5G-RRC Connection Setup Procedure**

1. UE detects Synchronization Signal (SS) to match DL synchronization. The UE gets system information (MIB), and measures Beam Reference Signal (BRS) to find DL beam pair. The UE receives system information (SIB).

2. The UE send RACH preamble to 5G RAN.

3. The 5G RAN sends Random Access Response to the UE.

4. The UE sends RRC Connection Request to the 5G RAN.

5. The 5G RAN sends RRC Connection Setup to the UE.

NOTE: SRB1 shall be established between UE and 5G RAN after the UE receives RRC Connection Setup message.

6. The UE replies RRC Connection Setup Complete message to the 5G RAN.

7. The 5G RAN sends RRC Connection Reconfiguration message to the UE.

8. The UE replies RRC Connection Reconfiguration Complete message to the 5G RAN.

## **6 RAN-CN signalling and user plane: NG1-C and NG1-U**

---

This sub clause provides an overview of functionalities supported by NG1-C and NG1-U. This is classified into wireless control and networking functions.

Wireless Control functions:

- Mobility Functions for UEs in connected mode (to cope with RF changes);
- NAS Signalling Transport function;

- NG1-C-interface management functions;
- Location Information reporting (details FFS);
- Context management functions.

Networking functions:

- User plane management function;
  - Setup, Modify, Release.
- 3 User plane (PDN) connections should be supported.

Note: the choice of user plane protocol and tunnelling is chosen under the circumstances specification has to be delivered prior to June for FWA use case. This may be revisited after June 2016.

UE and Network are expected to support three PDN connections for Fixed Wireless use case. It is agreed that mobility and IP anchoring functionality is required in the core network. Core Network will act as an IP anchor point for the PDN connections. It is also agreed there is no need for IP anchor function relocation procedures in the initial FWA specification.

Anchoring functionality in the RAN alone is insufficient. While the RG is expected to remain stationary, it is anticipated that environmental changes trigger handovers between RAN nodes with associated IP address changes as RAN coverage oscillates between RAN domains (fades, precipitation, foliage changes, or new billboard). These oscillations are present even assuming stationary residential gateways and RAN-hosted mobility anchors.

NG1-U supports GTP-U protocol stack as in 3GPP TS 29.281.

NG1-C support S1AP signalling transport as defined in 3GPP TS 36.412 with the following exceptions:

- SCTP Payload Protocol Identifier 32786 is used instead of 18
- Destination Port Number 50412 is used instead of 36412.



## 7 5G L2 user plane

---

5G Layer 2 is split into the following sublayers: 5G Medium Access Control (5G-MAC), 5G Radio Link Control (5G-RLC), and 5G Packet Data Convergence Protocol (5G-PDCP).

This subclause gives a high level description of the 5G layer 2 sub-layers in terms of services and functions.

### 7.1 5G Medium Access Control

This subclause provides an overview on services and functions provided by the 5G-MAC sublayer.

#### 7.1.1 Services and Functions

The main services and functions of the 5G-MAC sublayer include:

- Beam management;
- Random access procedure;
- Mapping between logical channels and transport channels;
- Concatenation of multiple MAC SDUs belonging to one logical channel into transport block (TB)
- Multiplexing/demultiplexing of 5G-MAC SDUs belonging to one or different logical channels into/from transport blocks (TB) delivered to/from the physical layer on transport channels;
- Scheduling information reporting;
- Error correction through HARQ;
- Priority handling between logical channels of one UE;
- Priority handling between UEs by means of dynamic scheduling;
- Transport format selection;
- Padding.

#### 7.1.2 Logical Channels

Different kinds of data transfer services as offered by 5G-MAC. Each logical channel type is defined by what type of information is transferred.

A general classification of logical channels is into two groups:

- Control Channel (for the transfer of control plane information);
- Traffic Channels (for the transfer of user plane information).

The 5G MAC entity can be configured with multiple cells which can be aggregated up to 7 secondary cells in addition to the primary cell. 5G-MAC generally consists of several function blocks (transmission

scheduling functions, per UE functions, 5G-MAC control functions, transport block generation). Transparent Mode is only applied to xBCCH.

### 7.1.2.1 Control Channel

Control channels are used for transfer of control plane information only. The control channels offered by 5G-MAC are:

- **5G Broadcast Control Channel (xBCCH)**

A downlink channel for broadcasting 5G system control information.

- **5G Common Control Channel (xCCCH)**

Channel for transmitting control information between UEs and network. This channel is used for UEs having no 5G-RRC connection with the network.

- **5G Dedicated Control Channel (xDCCH)**

A point-to-point bi-directional channel that transmits dedicated control information between a UE and the network. Used by UEs having a 5G-RRC connection.

### 7.1.2.2 Traffic Channels

Traffic channel is used for the transfer of user plane information only. The traffic channel offered by 5G-MAC is:

- **5G Dedicated Traffic Channel (xDTCH)**

A 5G Dedicated Traffic Channel (xDTCH) is a point-to-point channel, dedicated to one UE, for the transfer of user information. A xDTCH can exist in both uplink and downlink.

## 7.1.3 Mapping between logical channels and transport channels

### 7.1.3.1 Mapping in Uplink

The figure below depicts the mapping between uplink logical channels and uplink transport channels:

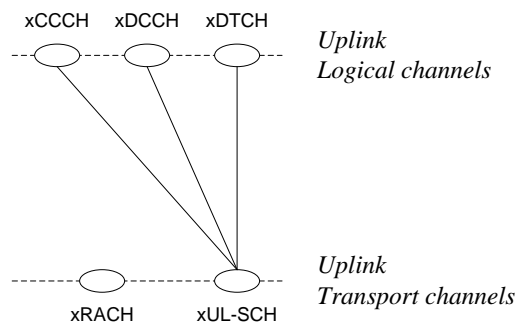


Figure 7.1.3.1-1: Mapping between uplink logical channels and uplink transport channels

In Uplink, the following connections between logical channels and transport channels exist:

- xCCCH can be mapped to xUL-SCH;
- xDCCH can be mapped to xUL-SCH;
- xDTCH can be mapped to xUL-SCH.

### 7.1.3.2 Mapping in Downlink

The figure below depicts the mapping between downlink logical channels and downlink transport channels:

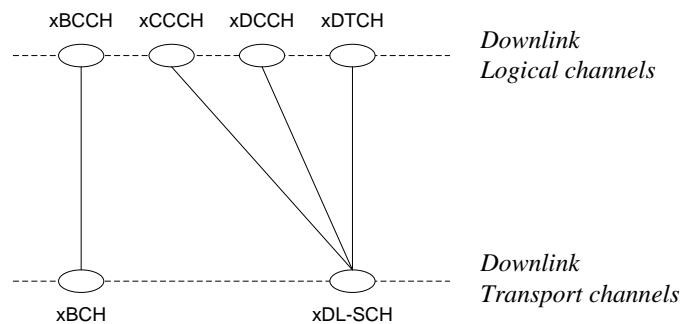


Figure 7.1.3.2-1: Mapping between downlink logical channels and downlink transport channels

In Downlink, the following connections between logical channels and transport channels exist:

- xBCCH can be mapped to xBCH;
- xCCCH can be mapped to xDL-SCH;
- xDCCH can be mapped to xDL-SCH;
- xDTCH can be mapped to xDL-SCH.

### 7.1.4 PDU Structure

The MAC PDU structure supports MAC subheader with Logical Channel Identifier (LCID) of 5 bits, an E field of 1 bit and 16 bit length field for indicating length of MAC SDU. MAC CEs are identified by LCID.

## 1 7.2 5G Radio Link Control

---

This subclause provides an overview on services, functions and PDU structure provided by the 5G-RLC sublayer. Note that:

- The reliability of 5G-RLC is configurable: some radio bearers may tolerate rare losses (e.g. TCP traffic);
- Radio Bearers are characterized by a variable sized data unit.

The RLC protocol supports following modes

- Transparent mode
- Unacknowledged mode
- Acknowledged mode

### 7.2.1 Services and Functions

The main services and functions of the 5G-RLC sublayer include:

- Transfer of upper layer PDUs;
- Error Correction through ARQ (only for AM data transfer);
- Reordering of 5G-RLC data PDUs (only for UM and AM data transfer);
- Duplicate detection (only for UM and AM data transfer);
- Protocol error detection (only for AM data transfer);
- 5G-RLC SDU discard (only for UM and AM data transfer);
- Segmentation (only for UM and AM data transfer);
- Resegmentation (only for AM data transfer);
- 5G-RLC re-establishment.

### 7.2.2 PDU Structure

Figure 7.2.2-1 below depicts the RLC PDU structure where:

- The PDU sequence number carried by the RLC header is independent of the SDU sequence number (i.e. PDCP sequence number);
- A dotted line in the RLC SDU indicates the occurrence of segmentation;
- Because RLC does not support concatenation and segmentation only occurs when needed the content of an RLC PDU can generally be described by the following relations:
  - 1 complete SDU<sub>i</sub>; or
  - 1 segment of SDU<sub>i</sub> .



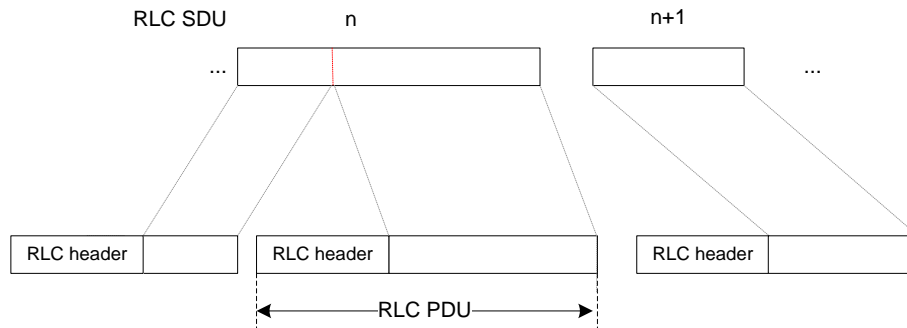


Figure 7.2.2-1: RLC PDU Structure

The RLC AM header contains Data/Control (D/C), Segmentation Flag (SF), Poll (P), Last Segment Flag (LSF) and Sequence Number (SN) fields.

The RLC UM header contains Segmentation Flag (SF), Last Segment Flag (LSF) and Sequence Number (SN) fields.

RLC AM and RLC UM use 18-bit SN.

### 7.3 5G Packet Data Convergence Protocol

This subclause provides an overview on services, functions and PDU structure provided by the 5G-PDCP sublayer.

#### 7.3.1 Services and Functions

The main services and functions of the 5G-PDCP sublayer for the user plane include:

- Transfer of user data;
- In-sequence delivery of upper layer PDUs at 5G-PDCP re-establishment procedure for 5G-RLC AM;
- Duplicate detection of lower layer SDUs at 5G-PDCP re-establishment procedure for 5G-RLC AM;
- Retransmission of 5G-PDCP SDUs at mobility in connected mode for 5G-RLC AM;
- Ciphering and deciphering;

Note: Only AES shall be mandatory

- Timer-based SDU discard in uplink.

The main services and functions of the 5G-PDCP for the control plane include:

- Ciphering and Integrity Protection;

Note: Only AES shall be mandatory

- Transfer of control plane data.

### 7.3.2 PDU Structure

Figure 7.3.2-1 below depicts the 5G-PDCP PDU structure for user plane data, where:

- 5G-PDCP PDU and 5G-PDCP header are octet-aligned;
- 5G-PDCP header is 3 bytes long;
- 5G-PDCP SN length for user plane data is 18 bits;
- The maximum supported size of a 5G-PDCP SDU is 65528 bytes.

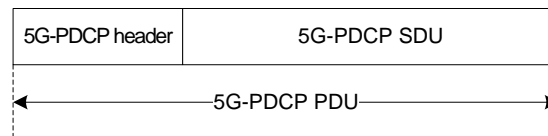


Figure 7.3.2-1: 5G-PDCP PDU Structure

The structures for control 5G-PDCP PDUs and for control plane 5G-PDCP data PDUs will be specified in 5G-PDCP stage 3 specification [VzW5G.323].

- 5G-PDCP SN length for control plane data is 18 bits.
- The maximum supported size of a 5G-PDCP SDU is 65528 bytes.

## 8 Mobility

---

### 8.1 Intra 5G-RAN

In 5G-RAN RRC\_CONNECTED state, mobility is based on a hybrid of network controlled and UE based procedures.

5GNB may configure separate measurements for

- detection of target cells for network controlled handover procedure
- detection of candidate cells for UE based handover procedure
- triggering of the handover execution in UE based handover procedure

In the first two cases, the UE reports detected cells normally based on measurement configuration.

The 5GNB may initiate the network controlled mobility procedure by transmitting RRC Connection Reconfiguration message containing mobility information with a single target cell for network controlled handover. Upon receiving the RRC Connection Reconfiguration message, the UE will make a random access attempt in the target cell. If the RRC Connection Reconfiguration message contained a dedicated random access resource, UE will use it for non-contention based random access.

The 5GNB may initiate the UE based mobility by transmitting RRC Connection Reconfiguration message containing mobility information with a list of candidate cells for UE based handover. The network will also configure a dedicated measurement event for handover execution in UE based handover procedure.

Upon triggering of this measurement event, the UE will attempt to perform a RRC Connection Reestablishment procedure in the best candidate cell.

Both network controlled and UE based mobility procedures may be initiated by the 5GNB without a prior measurement report from the UE.

If the UE is not able to connect to the target cell for network controlled mobility or to the best candidate cell for UE based mobility, a Radio Link Failure procedure is triggered.

Examples of the signalling sequences for mobility procedure are provided in Figures 8.1-1 to 8.1-4.

Figure 8.1-1 shows an example of a network controlled handover. The UE initially receives a measurement configuration (for network controlled handover) from 5GNB1 and performs signal quality measurements on BRSs from different cells of 5GNB1 and 5GNB2. Upon triggering of a measurement event, the UE transmits a measurement report to 5GNB1, which responds by transmitting a handover command (i.e. an RRC connection reconfiguration with target cell). The UE then accesses the target cell using received information. The procedure ends with RRC Connection Reconfiguration Complete

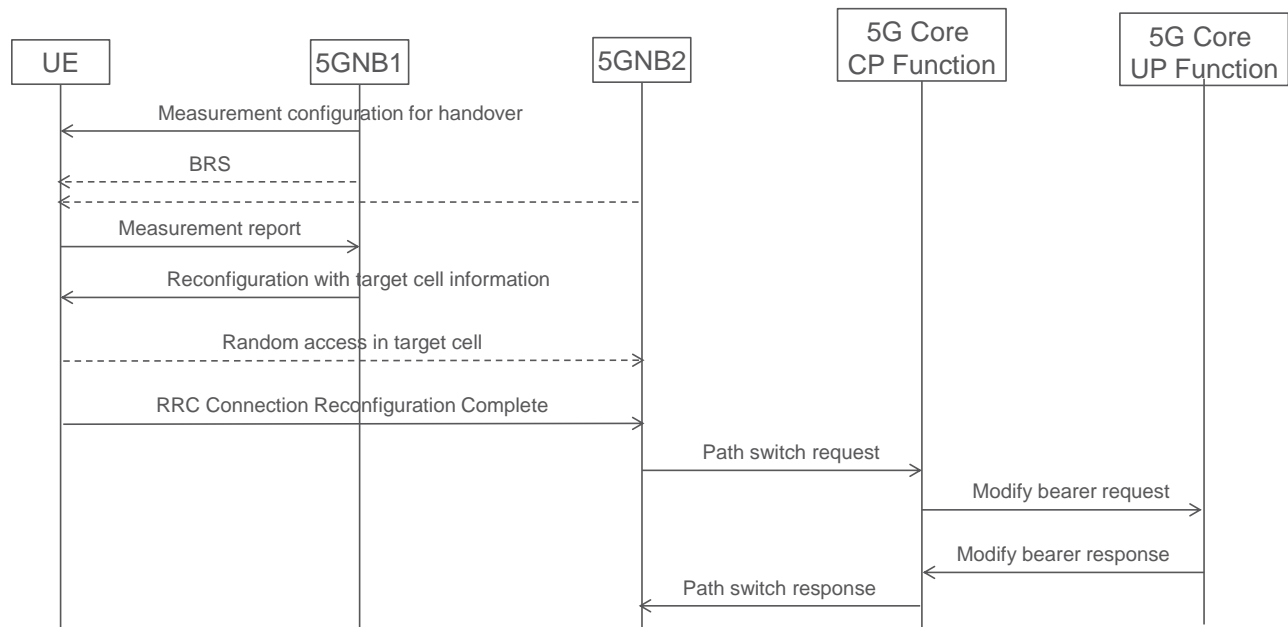


Figure 8.1-1: Example of network controlled handover

Figure 8.1-2 shows an example of a UE based handover. The UE initially receives a measurement configuration (for detection of candidate cells for UE based handover) from 5GNB1 and performs signal quality measurements on BRSs from different cells of 5GNB1 and 5GNB2. Upon triggering of the configured measurement event, the UE transmits a measurement report to 5GNB1, which responds by transmitting a list of candidate cells for UE based mobility (i.e. an RRC connection reconfiguration with list of target cells). The 5GNB1 also provides the UE with a measurement configuration for UE based handover execution. Upon triggering of the configured event for UE based handover execution, the UE then accesses the best candidate cell using RRC Connection Reestablishment procedure.

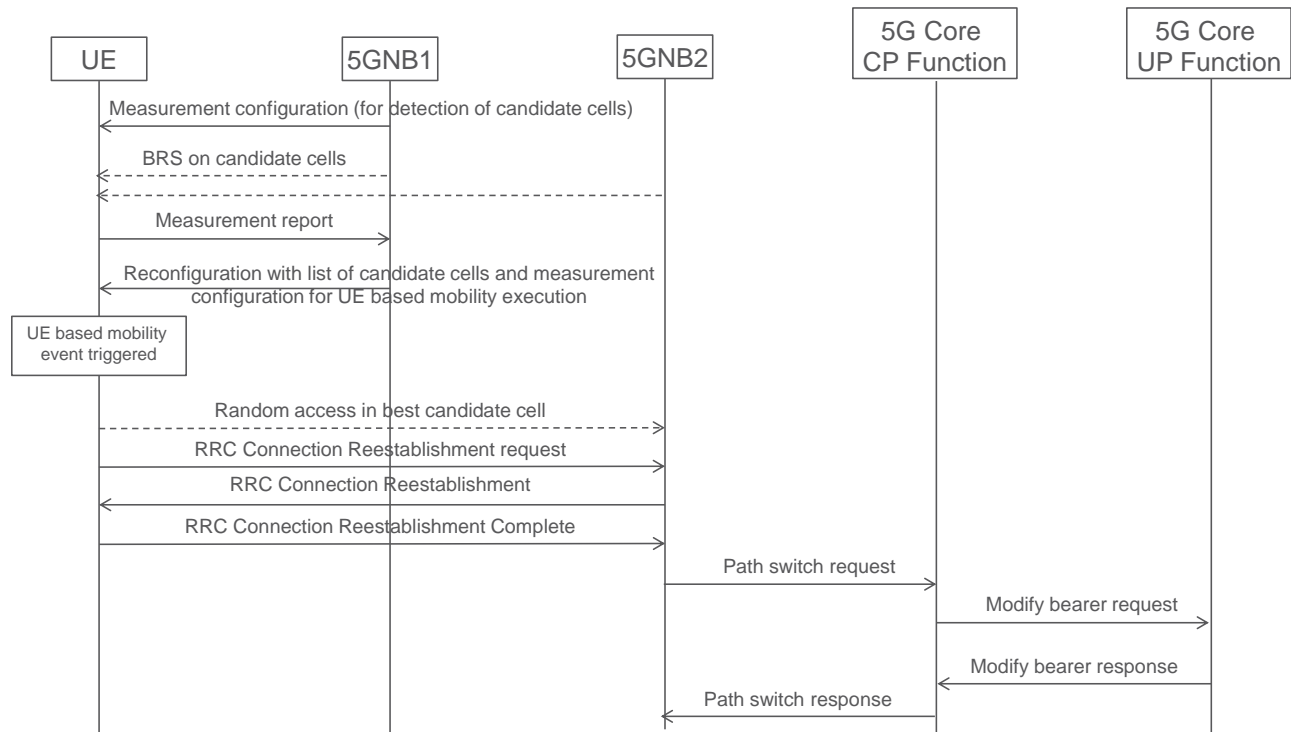


Figure 8.1-2: Example of UE based handover

Figure 8.1-3 shows an example of a joint operation of network controlled and UE based handover mechanisms. The UE initially receives a measurement configuration (for detection of candidate cells for UE based handover) from 5GNB1 and performs signal quality measurements on BRSs from different cells of 5GNB1 and 5GNB2. Upon triggering a measurement event, the UE transmits a measurement report to 5GNB1, which responds by transmitting a list of candidate cells for UE based mobility (i.e. an RRC connection reconfiguration with list of target cell). The 5GNB1 also provides the UE with a measurement configuration for UE based handover execution. The 5GNB1 also transmits a measurement configuration for network controlled mobility to the UE. However, before the UE can respond with a measurement report for network controlled mobility, the event for UE based handover execution is triggered, and the UE accesses the best candidate cell using RRC Connection Reestablishment procedure.

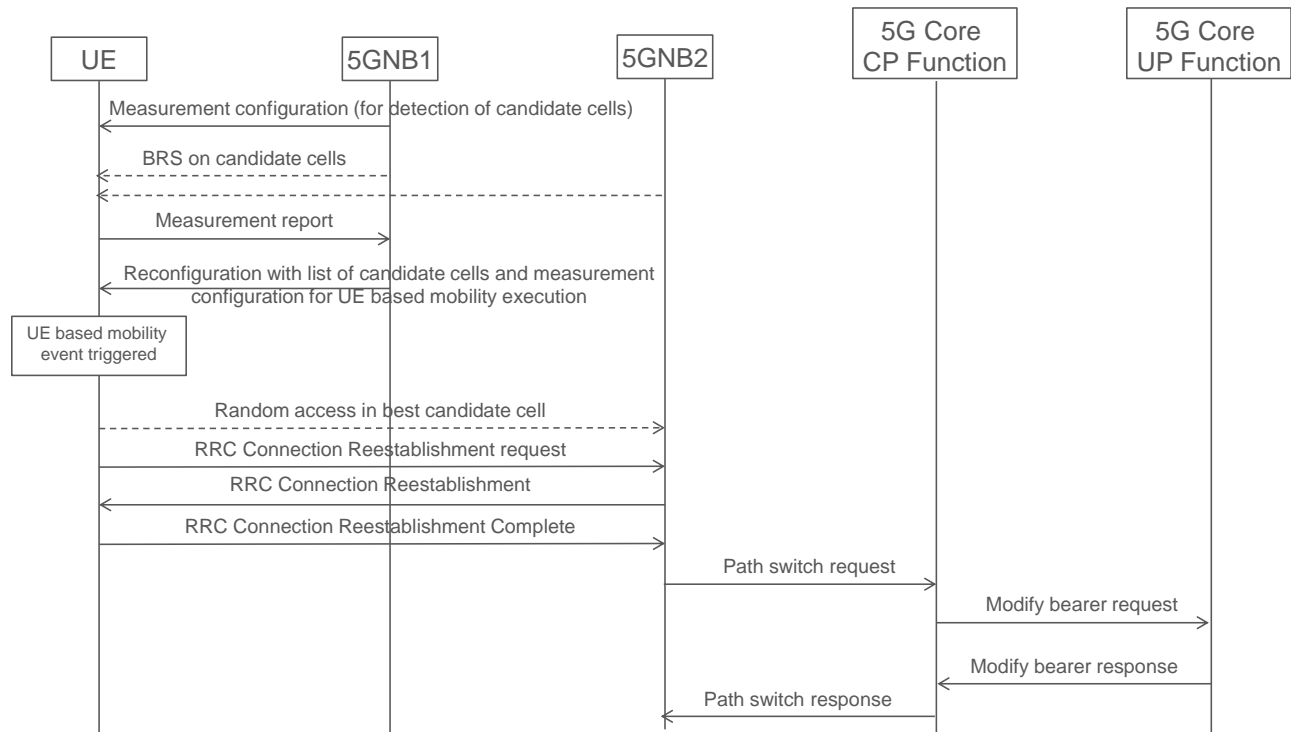


Figure 8.1-3: Example of joint operation of network controlled and UE based mobility procedures

## 8.2 Radio Link Failure

Two phases govern the behaviour associated to radio link failure as shown on Figure 8.2-1:

- First phase:
  - started upon radio problem detection - leads to radio link failure detection;
  - no UE-based mobility;
  - based on timer or other (e.g. counting) criteria ( $T_1$ ).
- Second Phase:
  - started upon radio link failure detection or handover failure;
  - leads to RRC\_IDLE;
  - UE-based mobility (i.e., cell selection);
  - Timer based ( $T_2$ ).

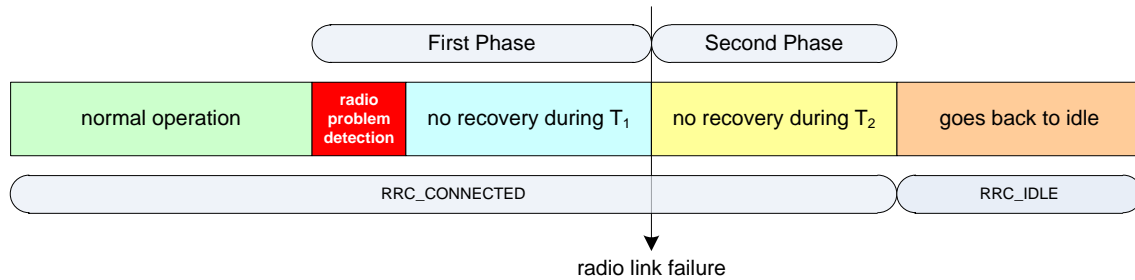


Figure 8.2-1: Radio Link Failure

In the Second Phase, in order to resume activity and avoid going via RRC\_IDLE when the UE returns to the same cell, following procedure applies (NOTE: The procedure when UE selects a different cell is FFS):

- The UE stays in RRC\_CONNECTED;
- The UE accesses the cell through the random access procedure;
- The UE identifier used in the random access procedure for contention resolution (i.e. C-RNTI of the UE in the cell where the RLF occurred + physical layer identity of that cell + short MAC-I based on the keys of that cell) is used by the selected 5G-NB to authenticate the UE and check whether it has a context stored for that UE:
  - If the 5G-NB finds a context that matches the identity of the UE, it indicates to the UE that its connection can be resumed;
  - If the context is not found, RRC connection is released and UE initiates procedure to establish new RRC connection. In this case UE is required to go via RRC\_IDLE.

### 8.3 Measurements

The UE reports measurement information in accordance with the measurement configuration as provided by the 5G-NB. 5G-RRC provides the measurement configuration applicable for a UE in RRC\_CONNECTED by means of dedicated signalling.

The measurement configuration includes the following parameters:

1. **Measurement objects:** the objects on which the UE shall perform the measurements.
  - A measurement object is a single 5G carrier frequency.
2. **Reporting configurations:** a list of reporting configurations where each reporting configuration consists of the following:
  - Reporting criterion: the criterion that triggers the UE to send a measurement report. This can either be periodical or a single event description. Five events are used:
    - Serving 5G cell becomes worse than threshold

- Neighbour 5G cell becomes offset better than serving 5G cell
- Serving 5G cell becomes better than threshold
- Neighbour 5G cell becomes better than threshold
- Serving 5G cell becomes worse than threshold1 and neighbour 5G cell becomes better than threshold2

NOTE: Layer 3 filtering is used.

3. **Quantity:** the measurement quantity for 5G carrier frequencies is RSRP.

5G-RRC only configures a single measurement object for a given 5G frequency, i.e. it is not possible to configure two or more measurement objects for the same frequency with different associated parameters. Multiple instances of the same event can be configured though e.g. by configuring two reporting configurations with different thresholds.

For instance, for the definition of intra frequency measurements, this means:

- Intra-frequency neighbour (cell) measurements: Neighbour cell measurements performed by the UE are intra-frequency measurements when one of the serving cells and the target cell operates on the same carrier frequency. The UE shall be able to carry out such measurements without measurement gaps.

## 9 ARQ and HARQ

---

5G RAN provides ARQ and HARQ functionality. The ARQ functionality provides error correction by retransmissions in acknowledged mode (AM) at 5G Layer 2. The HARQ functionality ensures delivery between peer entities at Layer 1.

### 9.1 HARQ principles

The HARQ within the 5G-MAC sublayer has the following characteristics:

- N-process Stop-And-Wait;
- HARQ transmits and retransmits transport blocks;
- In the downlink:
  - Asynchronous adaptive HARQ;

NOTE: in CC mode the adaptive only applies to the frequency allocation as specified in 5G.213.

- Uplink ACK/NAKs in response to downlink (re)transmissions are sent on xPUCCH or xPUSCH, which is configured by 5G RRC;
- xPDCCH signals the HARQ process number and if it is a transmission or retransmission (NDI is commonly applied to both codewords);

- UL feedback time on xPUCCH is configurable by an timing information signalled by xPDCCH , which is depended on UE capability associated with the minimum HARQ feedback processing time on UE side;
- The length of HARQ feedback reporting information is configurable by 5G RRC signalling by 5G Node;
- Retransmissions are always scheduled through xPDCCH.
- In the uplink:
  - Asynchronous adaptive HARQ;

NOTE: in CC mode the adaptive only applies to the frequency allocation as specified in 5G.213.

- Maximum number of retransmissions configured per UE (as opposed to per radio bearer);
- Downlink ACK/NAKs in response to uplink (re)transmissions are identified at UE with NDI and HARQ process number signalled by xPDCCH i.e. there is no explicit ACK/NACK information;
- xPDCCH signals the HARQ process number and if it is a transmission or retransmission (NDI is commonly applied to both codewords);
- Retransmissions are always scheduled through xPDCCH.

## 9.2 ARQ principles

The ARQ within the 5G-RLC sublayer has the following characteristics:

- ARQ retransmits 5G-RLC PDUs or 5G-RLC PDU segments based on 5G-RLC STATUS PDU;
- Polling for 5G-RLC STATUS PDU is used when needed by 5G-RLC;
- 5G-RLC receiver can also trigger 5G-RLC STATUS PDU after detecting a missing 5G-RLC PDU or 5G-RLC PDU segment.

## 10 Scheduling

---

In order to utilise the xSCH resources efficiently, a scheduling function is used in 5G-MAC. In this subclause, an overview of the scheduler is given in terms of scheduler operation, signalling of scheduler decisions, and measurements to support scheduler operation.

### 10.1 Basic Scheduler Operation

5G-MAC in 5G-NB includes dynamic resource schedulers that allocate physical layer resources for the xDL-SCH, xUL-SCH transport channels. Different schedulers operate for the xDL-SCH, xUL-SCH.

The scheduler should take account of the traffic volume and the QoS requirements of each UE and associated radio bearers, when sharing resources between UEs. Only "per UE" grants are used to grant the right to transmit on the xUL-SCH (i.e. there are no "per UE per RB" grants).



Schedulers may assign resources taking account the radio conditions at the UE identified through measurements made at the 5G-NB and/or reported by the UE.

Radio resource allocations can be valid for one TTI.

Resource assignment consists of physical resource blocks (PRBs) and MCS.

When CA is configured, a UE may be scheduled over multiple serving cells simultaneously but at most one random access procedure shall be ongoing at any time. Cross-carrier scheduling is not supported.

A linking between UL and DL allows identifying the serving cell for which the DL assignment or UL grant applies as follows:

- DL assignment received on PCell corresponds to downlink transmission on PCell;
- UL grant received on PCell corresponds to uplink transmission on PCell;
- DL assignment received on SCell<sub>n</sub> corresponds to downlink transmission on SCell<sub>n</sub>;
- UL grant received on SCell<sub>n</sub> corresponds to uplink transmission on SCell<sub>n</sub>. If SCell<sub>n</sub> is not configured for uplink usage by the UE, the grant is ignored by the UE.

### 10.1.1 Downlink Scheduling

In the downlink, 5G RAN can dynamically allocate resources (PRBs and MCS) to UEs at each TTI via the C-RNTI on xPDCCH(s). A UE always monitors the xPDCCH(s) in order to find possible allocation when its downlink reception is enabled. When CA is configured, the same C-RNTI applies to all serving cells.

When required, retransmissions are explicitly signalled via the xPDCCH(s).

### 10.1.2 Uplink Scheduling

In the uplink, 5G RAN can dynamically allocate resources (PRBs and MCS) to UEs at each TTI via the C-RNTI on xPDCCH(s). A UE always monitors the xPDCCH(s) in order to find possible allocation for uplink transmission when its downlink reception is enabled. When CA is configured, the same C-RNTI applies to all serving cells.

Retransmissions are explicitly allocated via xPDCCH(s).

NOTE: when the UE does not have enough data to fill the allocated resource, padding is used.

## 10.2 Measurements to Support Scheduler Operation

Measurement reports are required to enable the scheduler to operate in both uplink and downlink. These include transport volume and measurements of a UE's radio environment.

Uplink buffer status reports (BSR) are needed to provide support for QoS-aware packet scheduling. In 5G RAN uplink buffer status reports refer to the data that is buffered in for a group of logical channel (LCG) in the UE. The number of LCGs is FFS. One format is used for reporting in uplink:

- One BSR format is supported;

Uplink buffer status reports are transmitted using 5G-MAC signalling.

## 11 Carrier Aggregation

---

### 11.1 Principles

When CA is configured, the UE only has one 5G-RRC connection with the network. At 5G-RRC connection re-establishment/handover, one serving cell provides the security input. This cell is referred to as the Primary Cell (PCell).

Depending on UE capabilities, Secondary Cells (SCells) can be configured to form together with the PCell a set of serving cells. The configured set of serving cells for a UE therefore always consists of one PCell and one or more SCells:

- From a UE viewpoint, each uplink resource only belongs to the corresponding serving cell;
- The number of serving cells that can be configured depends on the aggregation capability of the UE;
- PCell can only be changed with handover procedures (i.e. with security key change and 5G random access procedure);
- xPUCCH is configured on each serving cell;
- Re-establishment is triggered when PCell experiences RLF, not when SCells experience RLF;
- NAS information is taken from PCell.

The reconfiguration, addition and removal of SCells can be performed by 5G-RRC signalling. At handover, 5G-RRC can also add, remove, or reconfigure SCells for usage with the target PCell. When adding a new SCell, dedicated 5G-RRC signalling is used for sending all required system information of the SCell i.e. while in 5G-RRC\_CONNECTED, UEs need not acquire broadcasted system information directly from the SCells. The SCells are initially activated upon addition and after handover.

### 11.2 Layer 2 Structure

In case of CA, the multi-carrier nature of the physical layer is only exposed to the 5G-MAC layer for which one HARQ entity is required per serving cell;

- In both uplink and downlink, there is one independent hybrid-ARQ entity per serving cell and one transport block is generated per TTI per serving cell in the absence of spatial multiplexing. Each transport block and its potential HARQ retransmissions are mapped to a single serving cell.

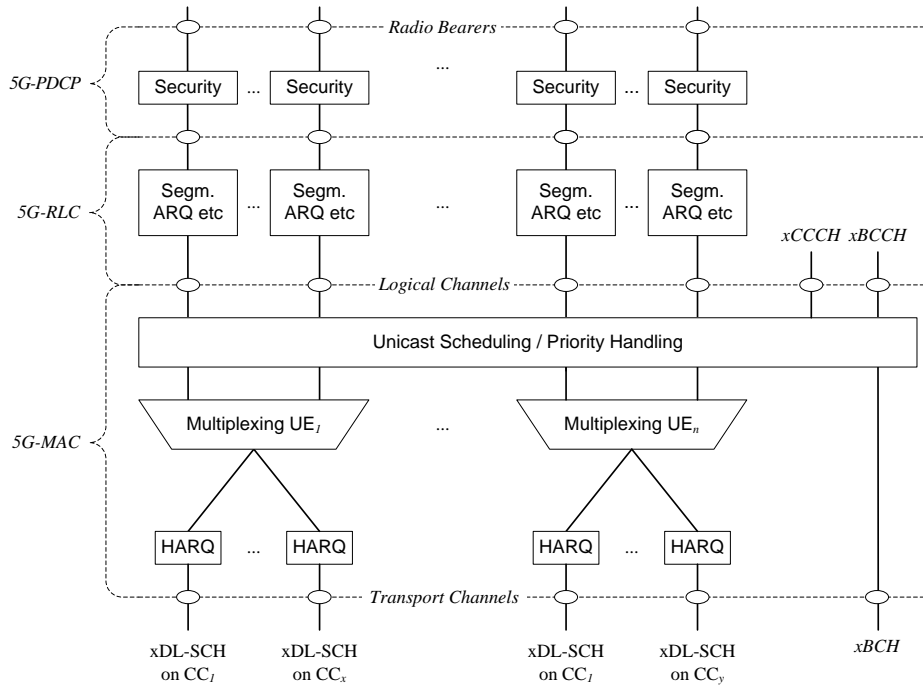


Figure 11.2-1: 5G Layer 2 Structure for DL with CA configured

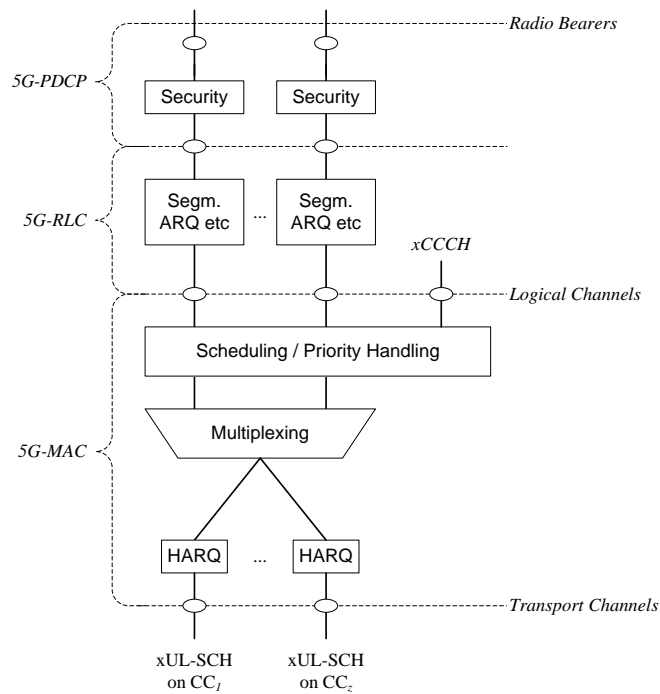


Figure 11.2-2: 5G Layer 2 Structure for UL with CA configured

## 14 Security

---

### 14.1 Overview and Principles

The same security framework as in LTE is used for the Verizon 5G radio network AS security (see 3GPP TS 36.300 and TS 33.401).

**Editor's note:** Since we agreed on removing NAS security feature in this document, NAS security feature is out of scope in this document. So we have to decide later whether NAS security should be included or not for coincidences with LTE framework as in 3GPP TS 36.300.

NOTE : Only AES shall be mandatory, other algorithms could be considered for subsequent phases.

The following principles apply to Verizon 5G radio network AS security:

- The 5GNB keys are cryptographically separated from the 5G CN keys used for NAS protection (making it impossible to use the 5G NB key to figure out a 5G CN key).
- The AS (RRC and UP) keys are derived in the 5G CN/UE from key material that was generated by a NAS (5G CN/UE) level AKA procedure ( $K_{ASME}$ ) and identified with a key identifier ( $KSI_{ASME}$ ).
- The 5G NB key ( $K_{5G-NB}$ ) is sent from the 5G CN to the 5G NB when the UE is entering RRC-CONNECTED state (i.e. during RRC connection or NG1 context setup).
- AS level security mode command procedure configures AS security (RRC and user plane). Both integrity protection and ciphering for RRC are activated within the same AS SMC procedure. User plane ciphering is activated at the same time as RRC ciphering.
- Keys stored inside 5G NBs shall never leave a secure environment within the 5G NB (except when done in accordance with this or other 3GPP specifications), and user plane data ciphering/deciphering shall take place inside the secure environment where the related keys are stored.
- A sequence number (COUNT) is used as input to the ciphering and integrity protection. A given sequence number must only be used once for a given 5G NB key (except for identical re-transmission) on the same radio bearer in the same direction. The same sequence number can be used for both ciphering and integrity protection.
- A hyper frame number (HFN) (i.e. an overflow counter mechanism) is used in the 5G NB and UE in order to limit the actual number of sequence number bits that is needed to be sent over the radio. The HFN needs to be synchronized between the UE and 5G NB.

A simplified key derivation is depicted on Figure 14.1-1 below, where:

**Editor's note:** dotted line in Figure 14.1-1 is for NAS security key derivation, which is out of scope of this document.

- $K_{5G-NB}$  is a key derived by UE and MSM from  $K_{ASME}$ .  $K_{5G-NB}$  may also be derived by the target 5GNB from NH at handover.  $K_{5G-NB}$  shall be used for the derivation of  $K_{RRCint}$ ,  $K_{RRCenc}$  and  $K_{UPenc}$ , and for the derivation of  $K_{5G-NB^*}$  upon handover.

- $K_{5G-NB}^*$  is a key derived by UE and 5G NB from  $K_{5G-NB}$ .  $K_{5G-NB}^*$  shall be used by UE and 5G NB as a new  $K_{5G-NB}$  for RRC and UP traffic.
- $K_{UPenc}$  is a key, which shall only be used for the protection of UP traffic with a particular encryption algorithm. This key is derived by UE and 5G NB from  $K_{5G-NB}$ , as well as an identifier for the encryption algorithm.
- $K_{RRCint}$  is a key, which shall only be used for the protection of RRC traffic with a particular integrity algorithm.  $K_{RRCint}$  is derived by UE and 5G NB from  $K_{5G-NB}$ , as well as an identifier for the integrity algorithm.
- $K_{RRCenc}$  is a key, which shall only be used for the protection of RRC traffic with a particular encryption algorithm.  $K_{RRCenc}$  is derived by UE and 5G NB from  $K_{5G-NB}$  as well as an identifier for the encryption algorithm.
- Next Hop (**NH**) is used by UE and 5GNB in the derivation of  $K_{5GNB}^*$  for the provision of "forward security". NH is derived by UE and MSM from  $K_{ASME}$  and  $K_{5GNB}$  when the security context is established, or from  $K_{ASME}$  and previous NH, otherwise.
- Next Hop Chaining Count (**NCC**) is a counter related to NH (i.e. the amount of Key chaining that has been performed) which allow the UE to be synchronised with the 5GNB and to determine whether the next  $K_{5GNB}^*$  needs to be based on the current  $K_{5GNB}$  or a fresh NH.

Editor's note: The USIM based security framework needs to be confirmed.

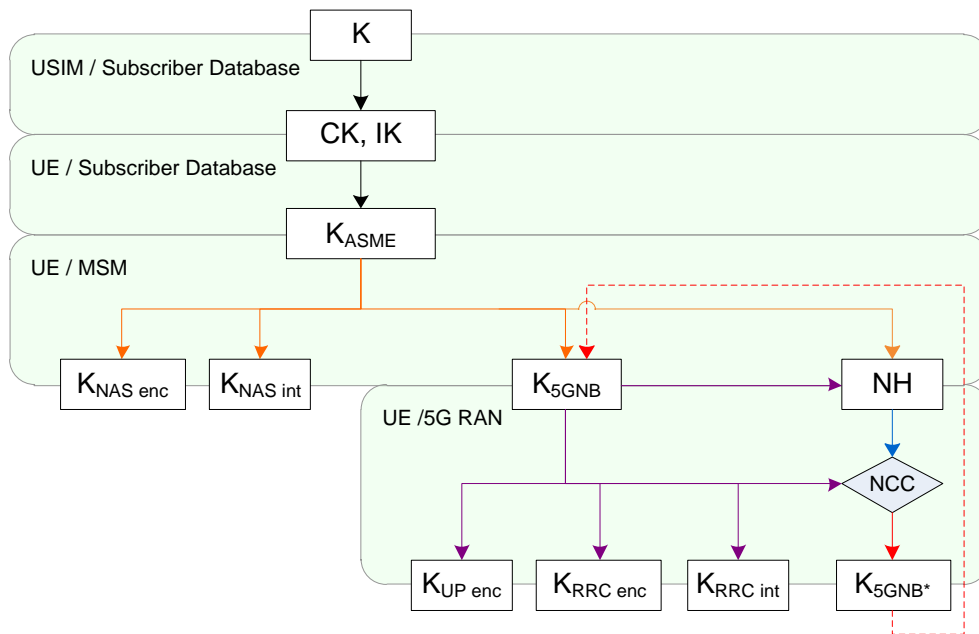


Figure 14.1-1: Key Derivation

## 14.2 Security termination points

The table below describes the security termination points.

Table 14.2-1 Security Termination Points

	<b>Ciphering</b>	<b>Integrity Protection</b>
U-Plane Data	Required and terminated in 5G NB	Not Required (NOTE 1)
RRC Signalling (AS)	Required and terminated in 5G NB	Required and terminated in 5G NB
MAC Signalling (AS)	Not required	Not required
NOTE 1: Integrity protection for U-Plane is not required and thus it is not supported between UE and uGW or for the transport of user plane data between 5G NB and uGW on NG1 interface.		

### 14.3 State Transitions and Mobility

#### 14.3.1 RRC\_IDLE to RRC\_CONNECTED

As a general principle, on RRC\_IDLE to RRC\_CONNECTED transitions, RRC protection keys and UP protection keys shall be generated while keys for NAS protection as well as higher layer keys are assumed to be already available in the MSM. These higher layer keys may have been established in the MSM as a result of an AKA run, or as a result of a transfer from another MSM during handover.

#### 14.3.2 RRC\_CONNECTED to RRC\_IDLE

On RRC\_CONNECTED to RRC\_IDLE transitions, 5GNBs shall delete the keys they store such that state for idle mode UEs only has to be maintained in MSM. It is also assumed that 5GNB does no longer store state information about the corresponding UE and deletes the current keys from its memory. In particular, on connected to idle transitions:

- The 5GNB and UE deletes NH, K5GNB, KRRCenc, KRRCint and KUPenc and related NCC.
- MSM and UE keeps KASME, KNASint and KNASenc stored.

#### 14.3.3 Intra 5G RAN Mobility

The key hierarchy does not allow, as is, explicit RRC and UP key updates, but RRC and UP keys are derived based on the algorithm identifiers and K5GNB which results with new RRC and UP keys at every handover:

- Source 5GNB and UE independently create K5GNB\* with the input parameters
- K5GNB\* is given to Target 5GNB during the HO preparation phase;
- Both Target 5GNB and UE considers the new K5GNB equal to the received K5GNB\*.

### 14.4 AS Key Change in RRC\_CONNECTED