TS 5G.323 V1.0 (2016-06)

Technical Specification

KT PyeongChang 5G Special Interest Group (KT 5G-SIG);
KT 5th Generation Radio Access;
Packet Data Convergence Protocol (PDCP);
Protocol specification
(Release 1)

Ericsson, Intel Corp., Nokia, Qualcomm Technologies Inc., Samsung Electronics & KT

Disclaimer: This document provides information related to 5G technology. All information provided herein is subject to change without notice. The members of the KT PyeongChang 5G Special Interest Group ("KT 5G-SIG") disclaim and make no guaranty or warranty, express or implied, as to the accuracy or completeness of any information contained or referenced herein. THE KT 5G-SIG 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 KT 5G-SIG 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 KT 5G-SIG and its members disclaim liability for any damages or losses of any nature whatsoever whether direct, indirect, incidental, special or consequential resulting from the use of or reliance on any information contained or referenced herein.

Document History

Version	Date	Change
0.1	2016-04-29	First Draft Version
1.0	2016-07-13	Final Version

Contents

Foreword

This Technical Specification has been produced by the KT PyeongChang 5G Special Interest Group (KT 5G-SIG).

1 Scope

The present document provides the description of the Packet Data Convergence Protocol (PDCP) for the PyeongChang 5G trial (P5G).

2 References

[1] TS 5G.300: “PyeongChang 5th Generation Radio Access;Overall Description”.

[2] TS 5G.331: “5G Radio Access (5G RA); Resource Control (5G-RRC); Protocol Specification”.

[3] TS 5G.322: “5G Radio Access (5G RA); Radio Link Control (5G-RLC) protocol specification”.

[4] TS 5G.321: “5G Radio Access (5G RA); Medium Access Control (5G-MAC) protocol specification”.

[5] 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.

3.2 Abbreviations

AM	Acknowledged Mode
ARP	Address Resolution Protocol
CID	Context Identifier
DRB	Data Radio Bearer carrying user plane data
EPS	Evolved Packet System
5G Node-B	5G Node B
5G RA	5G Radio Access
5G RAN	5G Radio Access Network
xDTCH	5G Dedicated Traffic Channel
FMS	First missing PDCP SN
HFN	Hyper Frame Number
IETF	Internet Engineering Task Force
IP	Internet Protocol
L2	Layer 2 (data link layer)
L3	Layer 3 (network layer)
MAC	Medium Access Control
MAC-I	Message Authentication Code for Integrity
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
R	Reserved
RB	Radio Bearer
RLC	Radio Link Control
RRC	Radio Resource Control
SAP	Service Access Point
SDU	Service Data Unit
SN	Sequence Number
SRB	Signalling Radio Bearer carrying control plane data
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

UE	User Equipment
UM	Unacknowledged Mode
X-MAC	Computed MAC-I

4 General

4.1 Introduction

The present document describes the functionality of the PDCP. The functionality specified for the UE applies to communication on Uu interface

4.2 PDCP architecture

4.2.1 PDCP structure

Figure 4.2.1.1 represents one possible structure for the PDCP sublayer; it should not restrict implementation. The figure is based on the radio interface protocol architecture defined in [1].

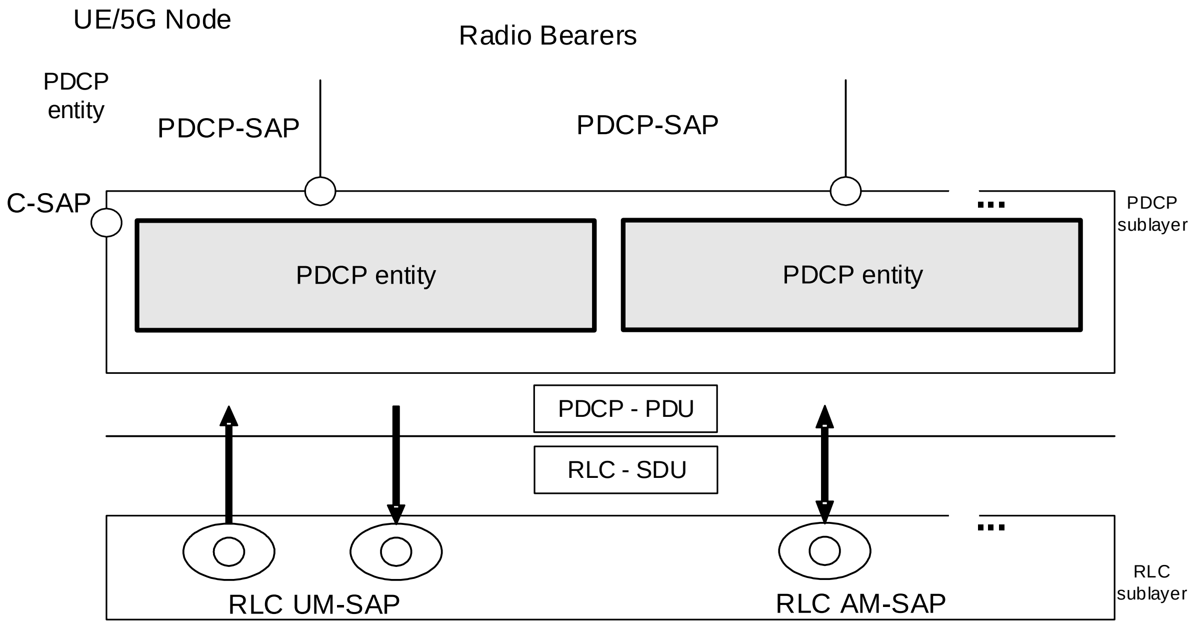


Figure 4.2.1.1 - PDCP layer, structure view

Each RB (i.e. DRB,) is associated with one PDCP entity, whereas in standalone mode each RB (i.e. DRB, and SRB, except for SRB0) is associated with one PDCP entity. Each PDCP entity is associated with one or two (one for each direction) RLC entities depending on RLC mode.. The PDCP entities are located in the PDCP sublayer.

The PDCP sublayer is configured by upper layers [2].

4.2.2 PDCP entities

The PDCP entities are located in the PDCP sublayer. Several PDCP entities may be defined for a UE.

Each PDCP entity is carrying the data of one radio bearer.

Figure 4.2.2.1 represents the functional view of the PDCP entity for the PDCP sublayer, and Figure 4.2.2.1a represents the functional view of the PDCP entity for the PDCP sublayer in standalone mode; it should not restrict implementation. The figure is based on the radio interface protocol architecture defined in [1].

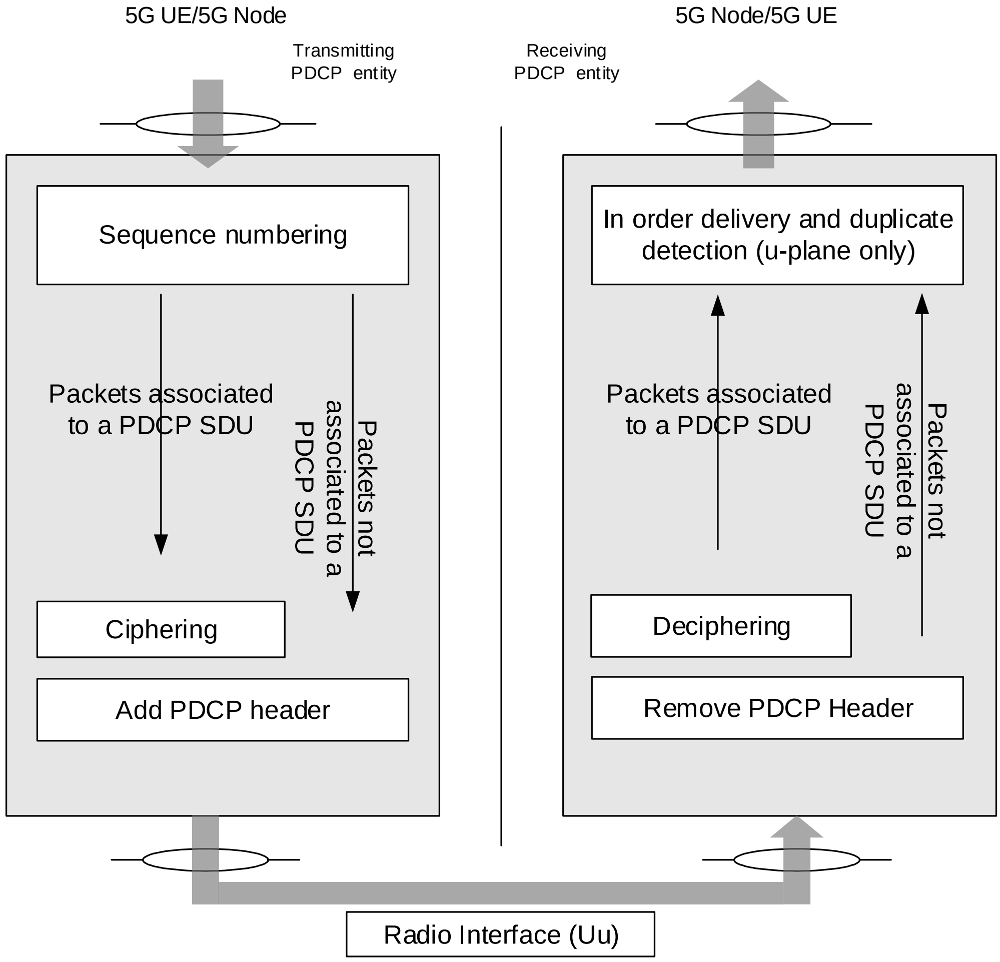

5G UE/5G Node
Transmitting PDCP entity
Receiving PDCP entity
5G Node/5G UE
Sequence numbering
Packets associated to a PDCP SDU
Packets not associated to a PDCP SDU
Ciphering
Add PDCP header
In order delivery and duplicate detection (u-plane only)
Packets associated to a PDCP SDU
Packets not associated to a PDCP SDU
Deciphering
Remove PDCP Header
Radio Interface (Uu)

Figure 4.2.2.1 - PDCP layer, functional view

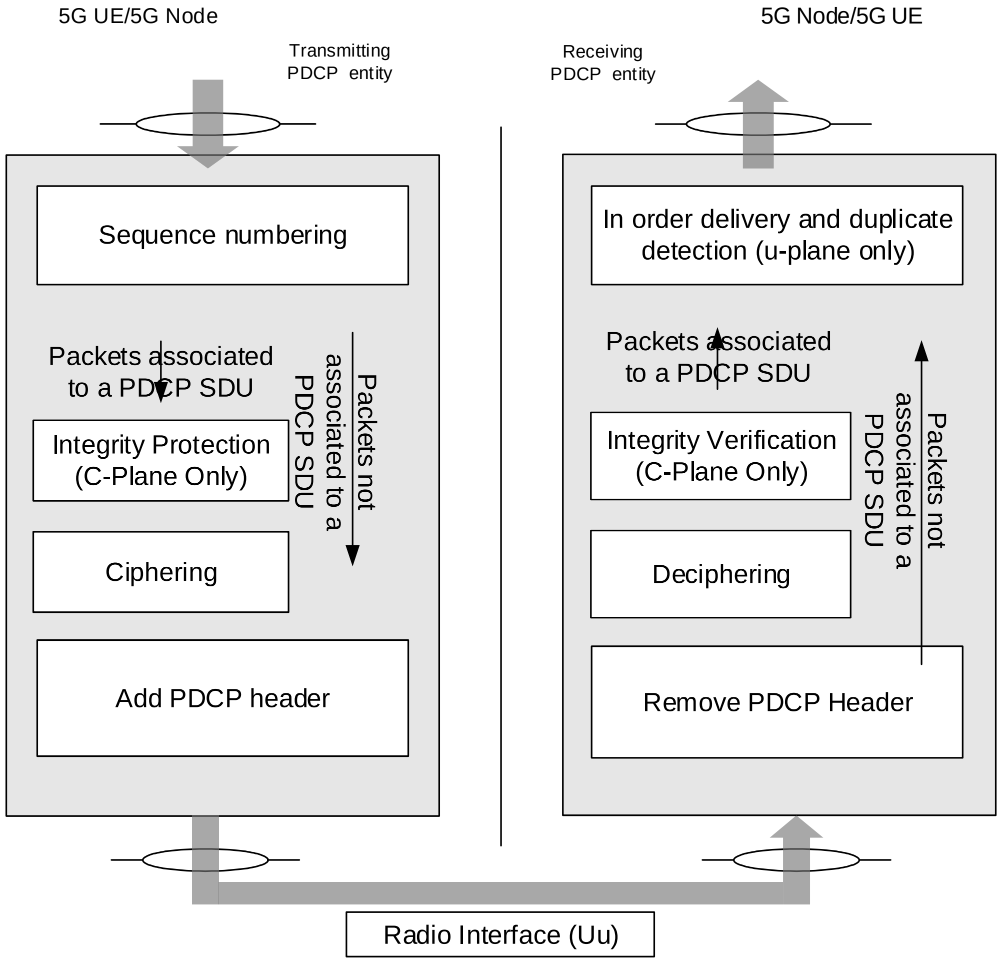

5G UE/5G Node
Transmitting PDCP entity
Receiving PDCP entity
5G Node/5G UE
Sequence numbering
Packets associated to a PDCP SDU
Packets not associated to a PDCP SDU
Integrity Protection (C-Plane Only)
Ciphering
Add PDCP header
In order delivery and duplicate detection (u-plane only)
Packets associated to a PDCP SDU
Packets not associated to a PDCP SDU
Integrity Verification (C-Plane Only)
Deciphering
Remove PDCP Header
Radio Interface (Uu)

Figure 4.2.2.1a - PDCP layer, functional view in standalone mode

4.3 Services

4.3.1 Services provided to upper layers

PDCP provides its services to the RRC and user plane upper layers at the UE The following services are provided by PDCP to upper layers:

- transfer of user plane data;
- transfer of control plane data (applicable only in standalone mode) ;
- ciphering;
- integrity protection (applicable only in standalone mode).

NOTE: only AES algorithm shall be mandatory

The maximum supported size of a PDCP SDU is 65528 octets. The maximum supported size of a PDCP Control PDU is 65528 octets.

4.3.2 Services expected from lower layers

A PDCP entity expects the following services from lower layers per RLC entity (for a detailed description see [3]):

- acknowledged data transfer service, including indication of successful delivery of PDCP PDUs;
- unacknowledged data transfer service;
- in-sequence delivery, except at re-establishment of lower layers;
- duplicate discarding, except at re-establishment of lower layers.

4.4 Functions

The Packet Data Convergence Protocol supports the following functions:

- transfer of data (user plane or control plane, where control plane is applicable only in standalone mode); maintenance of PDCP SNs;
- in-sequence delivery of upper layer PDUs at re-establishment of lower layers;
- duplicate elimination of lower layer SDUs at re-establishment of lower layers for radio bearers mapped on RLC AM;
- ciphering and deciphering of user plane data and control plane data;- In standalone mode ciphering and deciphering of user plane data and control plane data;
- integrity protection and integrity verification of control plane data, where it is applicable only in standalone mode;

NOTE: only AES algorithm shall be mandatory

- timer based discard;
- duplicate discarding;

PDCP uses the services provided by the RLC sublayer.

PDCP is used for DRBs, mapped on xDTCH type of logical channels. In standalone mode, PDCP is used for SRBs and DRBs mapped on xDCCH and xDTCH type of logical channels. PDCP is not used for any other type of logical channels.

4.5 Data available for transmission

For the purpose of MAC buffer status reporting, the UE shall consider PDCP Control PDUs, as well as the following as data available for transmission in the PDCP layer:

For SDUs for which no PDU has been submitted to lower layers:

- the SDU itself, if the SDU has not yet been processed by PDCP, or
- the PDU if the SDU has been processed by PDCP.

In addition, for radio bearers that are mapped on RLC AM, if the PDCP entity has previously performed the re-establishment procedure, the UE shall also consider the following as data available for transmission in the PDCP layer:

For SDUs for which a corresponding PDU has only been submitted to lower layers prior to the PDCP re-establishment, starting from the first SDU for which the delivery of the corresponding PDUs has not been confirmed by the lower layer, except the SDUs which are indicated as successfully delivered by the PDCP status report, if received:

- the SDU, if it has not yet been processed by PDCP, or
- the PDU once it has been processed by PDCP.

5 PDCP procedures

5.1 PDCP Data Transfer Procedures

5.1.1 UL Data Transfer Procedures

At reception of a PDCP SDU from upper layers, the UE shall:

- start the *discardTimer* associated with this PDCP SDU (if configured);

For a PDCP SDU received from upper layers, the UE shall:

- associate the PDCP SN corresponding to Next_PDCP_TX_SN to this PDCP SDU;

NOTE: Associating more than half of the PDCP SN space of contiguous PDCP SDUs with PDCP SNs, when e.g., the PDCP SDUs are discarded or transmitted without acknowledgement, may cause HFN desynchronization problem. How to prevent HFN desynchronization problem is left up to UE implementation.

- perform integrity protection (if applicable), and ciphering (if applicable) using COUNT based on TX_HFN and the PDCP SN associated with this PDCP SDU as specified in the subclause 5.7 and 5.6, respectively;
- increment Next_PDCP_TX_SN by one;
- if Next_PDCP_TX_SN > Maximum_PDCP_SN:
  - set Next_PDCP_TX_SN to 0;
  - increment TX_HFN by one;
- submit the resulting PDCP Data PDU to lower layer.

5.1.2 DL Data Transfer Procedures

5.1.2.1 Procedures for DRBs

5.1.2.1.1 Void

5.1.2.1.2 Procedures for DRBs mapped on RLC AM

For DRBs mapped on RLC AM at reception of a PDCP Data PDU from lower layers, the UE shall:

- if received PDCP SN – Last_Submitted_PDCP_RX_SN > Reordering_Window or 0 <= Last_Submitted_PDCP_RX_SN – received PDCP SN < Reordering_Window:
  - if received PDCP SN > Next_PDCP_RX_SN:
    - decipher the PDCP PDU as specified in the subclause 5.6, using COUNT based on RX_HFN - 1 and the received PDCP SN;
  - else:
    - decipher the PDCP PDU as specified in the subclause 5.6, using COUNT based on RX_HFN and the received PDCP SN;
  - discard this PDCP SDU;
- else if Next_PDCP_RX_SN – received PDCP SN > Reordering_Window:
  - increment RX_HFN by one;

  - use COUNT based on RX_HFN and the received PDCP SN for deciphering the PDCP PDU;
  - set Next_PDCP_RX_SN to the received PDCP SN + 1;
- else if received PDCP SN – Next_PDCP_RX_SN >= Reordering_Window:
  - use COUNT based on RX_HFN – 1 and the received PDCP SN for deciphering the PDCP PDU;
- else if received PDCP SN >= Next_PDCP_RX_SN:
  - use COUNT based on RX_HFN and the received PDCP SN for deciphering the PDCP PDU;
  - set Next_PDCP_RX_SN to the received PDCP SN + 1;
  - if Next_PDCP_RX_SN is larger than Maximum_PDCP_SN:
    - set Next_PDCP_RX_SN to 0;
    - increment RX_HFN by one;
- else if received PDCP SN < Next_PDCP_RX_SN:
  - use COUNT based on RX_HFN and the received PDCP SN for deciphering the PDCP PDU;
- if the PDCP PDU has not been discarded in the above:
  - perform deciphering for the PDCP PDU as specified in the subclauses 5.6;
  - if a PDCP SDU with the same PDCP SN is stored:
    - discard this PDCP SDU;
  - else:
    - store the PDCP SDU;
  - if the PDCP PDU received by PDCP is not due to the re-establishment of lower layers:
    - deliver to upper layers in ascending order of the associated COUNT value:
      - all stored PDCP SDU(s) with an associated COUNT value less than the COUNT value associated with the received PDCP SDU;
      - all stored PDCP SDU(s) with consecutively associated COUNT value(s) starting from the COUNT value associated with the received PDCP SDU;
    - set Last_Submitted_PDCP_RX_SN to the PDCP SN of the last PDCP SDU delivered to upper layers;.
  - else if received PDCP SN = Last_Submitted_PDCP_RX_SN + 1 or received PDCP SN = Last_Submitted_PDCP_RX_SN – Maximum_PDCP_SN:
    - deliver to upper layers in ascending order of the associated COUNT value:
      - all stored PDCP SDU(s) with consecutively associated COUNT value(s) starting from the COUNT value associated with the received PDCP SDU;
    - set Last_Submitted_PDCP_RX_SN to the PDCP SN of the last PDCP SDU delivered to upper layers.

5.1.2.1.3 Procedures for DRBs mapped on RLC UM

For DRBs mapped on RLC UM, at reception of a PDCP Data PDU from lower layers, the UE shall:

- if received PDCP SN < Next_PDCP_RX_SN:
  - increment RX_HFN by one;
- decipher the PDCP Data PDU using COUNT based on RX_HFN and the received PDCP SN as specified in the subclause 5.6;

- set Next_PDCP_RX_SN to the received PDCP SN + 1;
- if Next_PDCP_RX_SN > Maximum_PDCP_SN:
  - set Next_PDCP_RX_SN to 0;
  - increment RX_HFN by one;
- deliver the resulting PDCP SDU to upper layer.

5.1.2.2 Procedures for SRBs

NOTE: This procedure is applicable only in standalone mode

For SRBs, at reception of a PDCP Data PDU from lower layers, the UE shall:

- if received PDCP SN < Next_PDCP_RX_SN:
  - decipher and verify the integrity of the PDU (if applicable) using COUNT based on RX_HFN + 1 and the received PDCP SN as specified in the subclauses 5.6 and 5.7, respectively;
- else:
  - decipher and verify the integrity of the PDU (if applicable) using COUNT based on RX_HFN and the received PDCP SN as specified in the subclauses 5.6 and 5.7, respectively;
- if integrity verification is applicable and the integrity verification is passed successfully; or
- if integrity verification is not applicable:
  - if received PDCP SN < Next_PDCP_RX_SN:
    - increment RX_HFN by one;
  - set Next_PDCP_RX_SN to the received PDCP SN + 1;
  - if Next_PDCP_RX_SN > Maximum_PDCP_SN:
    - set Next_PDCP_RX_SN to 0;
    - increment RX_HFN by one;
  - deliver the resulting PDCP SDU to upper layer;
- else, if integrity verification is applicable and the integrity verification fails:
  - discard the received PDCP Data PDU;
  - indicate the integrity verification failure to upper layer.

.

5.2 Re-establishment procedure

When upper layers request a PDCP re-establishment, the UE shall additionally perform once the procedures described in this section for the corresponding RLC mode. After performing the procedures in this section, the UE shall follow the procedures in subclause 5.1.

5.2.1 UL Data Transfer Procedures

5.2.1.1 Procedures for DRBs mapped on RLC AM

When upper layers request a PDCP re-establishment, the UE shall:

- apply the ciphering algorithm and key provided by upper layers during the re-establishment procedure;

- from the first PDCP SDU for which the successful delivery of the corresponding PDCP PDU has not been confirmed by lower layers, perform retransmission or transmission of all the PDCP SDUs already associated with PDCP SNs in ascending order of the COUNT values associated to the PDCP SDU prior to the PDCP re-establishment as specified below:
  - perform ciphering of the PDCP SDU using the COUNT value associated with this PDCP SDU as specified in the subclause 5.6;
  - submit the resulting PDCP Data PDU to lower layer.

5.2.1.2 Procedures for DRBs mapped on RLC UM

When upper layers request a PDCP re-establishment, the UE shall:

- set Next_PDCP_TX_SN, and TX_HFN to 0;
- apply the ciphering algorithm and key provided by upper layers during the re-establishment procedure;
- for each PDCP SDU already associated with a PDCP SN but for which a corresponding PDU has not previously been submitted to lower layers:
  - consider the PDCP SDUs as received from upper layer;
  - perform transmission of the PDCP SDUs in ascending order of the COUNT value associated to the PDCP SDU prior to the PDCP re-establishment, as specified in the subclause 5.1.1 without restarting the *discardTimer*.

5.2.1.3 Procedures for SRBs

NOTE: This procedure is applicable only in standalone mode

When upper layers request a PDCP re-establishment, the UE shall:

- set Next_PDCP_TX_SN, and TX_HFN to 0;
- discard all stored PDCP SDUs and PDCP PDUs;
- apply the ciphering and integrity protection algorithms and keys provided by upper layers during the re-establishment procedure.

5.2.2 DL Data Transfer Procedures

5.2.2.1 Procedures for DRBs mapped on RLC AM

When upper layers request a PDCP re-establishment, the UE shall:

- process the PDCP Data PDUs that are received from lower layers due to the re-establishment of the lower layers, as specified in the subclause 5.1.2.1.2;
- apply the ciphering algorithm and key provided by upper layers during the re-establishment procedure.

5.2.2.2 Procedures for DRBs mapped on RLC UM

When upper layers request a PDCP re-establishment, the UE shall:

- process the PDCP Data PDUs that are received from lower layers due to the re-establishment of the lower layers, as specified in the subclause 5.1.2.1.3;
- set Next_PDCP_RX_SN, and RX_HFN to 0;
- apply the ciphering algorithm and key provided by upper layers during the re-establishment procedure.

5.2.2.3 Procedures for SRBs

NOTE: This procedure is applicable only in standalone mode

When upper layers request a PDCP re-establishment, the UE shall:

- discard the PDCP Data PDUs that are received from lower layers due to the re-establishment of the lower layers;
- set Next_PDCP_RX_SN, and RX_HFN to 0;
- discard all stored PDCP SDUs and PDCP PDUs;
- apply the ciphering and integrity protection algorithms and keys provided by upper layers during the re-establishment procedure.

5.3 PDCP Status Report

5.3.1 Transmit operation

When upper layers request a PDCP re-establishment, for radio bearers that are mapped on RLC AM, the UE shall:

- if the radio bearer is configured by upper layers to send a PDCP status report in the uplink (*statusReportRequired* [2]), compile a status report as indicated below after processing the PDCP Data PDUs that are received from lower layers due to the re-establishment of the lower layers as specified in the subclause 5.2.2.1, and submit it to lower layers as the first PDCP PDU for the transmission, by:
  - setting the FMS field to the PDCP SN of the first missing PDCP SDU;
  - if there is at least one out-of-sequence PDCP SDU stored, allocating a Bitmap field of length in bits equal to the number of PDCP SNs from and not including the first missing PDCP SDU up to and including the last out-of-sequence PDCP SDUs, rounded up to the next multiple of 8, or up to and including a PDCP SDU for which the resulting PDCP Control PDU size is equal to 65528 bytes, whichever comes first;
  - setting as ‘0’ in the corresponding position in the bitmap field for all PDCP SDUs that have not been received as indicated by lower layers, - indicating in the bitmap field as ‘1’ for all other PDCP SDUs.

5.3.2 Receive operation

When a PDCP status report is received in the downlink, for radio bearers that are mapped on RLC AM:

- for each PDCP SDU, if any, with the bit in the bitmap set to '1', or with the associated COUNT value less than the COUNT value of the PDCP SDU identified by the FMS field, the successful delivery of the corresponding PDCP SDU is confirmed, and the UE shall process the PDCP SDU as specified in the subclause 5.4.

5.4 PDCP discard

When the *discardTimer* expires for a PDCP SDU, or the successful delivery of a PDCP SDU is confirmed by PDCP status report, the UE shall discard the PDCP SDU along with the corresponding PDCP PDU. If the corresponding PDCP PDU has already been submitted to lower layers the discard is indicated to lower layers.

5.6 Ciphering and Deciphering

The ciphering function includes both ciphering and deciphering and is performed in PDCP. For the control plane, which is applicable only in standalone mode, the data unit that is ciphered is the data part of the PDCP PDU (see subclause 6.3.3) and the MAC-I (see subclause 6.3.4). For the user plane, the data unit that is ciphered is the data part of the PDCP PDU (see subclause 6.3.3); ciphering is not applicable to PDCP Control PDUs.

The ciphering algorithm and key to be used by the PDCP entity are configured by upper layers [2] and the ciphering method shall be applied as specified in [5].

The ciphering function is activated by upper layers [2]. After security activation, the ciphering function shall be applied to all PDCP PDUs indicated by upper layers [2] for the downlink and the uplink, respectively.

For downlink and uplink ciphering and deciphering, the parameters that are required by PDCP for ciphering are defined in [5] and are input to the ciphering algorithm. The required inputs to the ciphering function include the COUNT value, and DIRECTION (direction of the transmission: set as specified in [5]).The parameters required by PDCP which are provided by upper layers [2] are listed below:

- BEARER (defined as the radio bearer identifier in [5]. It will use the value RB identity –1 as in [2]);
- KEY (the ciphering keys for the control plane and for the user plane are 5G K_{RRCenc} and 5G K_{UPenc}, respectively).

5.7 Integrity Protection and Verification

NOTE: This procedure is applicable only in standalone modeThe integrity protection function includes both integrity protection and integrity verification and is performed in PDCP for PDCP entities associated with SRBs that needs integrity protection. The data unit that is integrity protected is the PDU header and the data part of the PDU before ciphering.

The integrity protection algorithm and key to be used by the PDCP entity are configured by upper layers [3] and the integrity protection method shall be applied as specified in [5].

The integrity protection function is activated by upper layers [3]. After security activation, the integrity protection function shall be applied to all PDUs including and subsequent to the PDU indicated by upper layers [3] for the downlink and the uplink, respectively.

NOTE: As the RRC message which activates the integrity protection function is itself integrity protected with the configuration included in this RRC message, this message needs first be decoded by RRC before the integrity protection verification could be performed for the PDU in which the message was received.

For downlink and uplink integrity protection and verification, the parameters that are required by PDCP for integrity protection are defined in [5] and are input to the integrity protection algorithm. The required inputs to the integrity protection function include the COUNT value, and DIRECTION (direction of the transmission: set as specified in [5]). The parameters required by PDCP which are provided by upper layers [3] are listed below:

- BEARER (defined as the radio bearer identifier in [5]. It will use the value RB identity –1 as in [3]);
- KEY (K_{RRCint}).

At transmission, the UE computes the value of the MAC-I field and at reception it verifies the integrity of the PDCP PDU by calculating the X-MAC based on the input parameters as specified above. If the calculated X-MAC corresponds to the received MAC-I, integrity protection is verified successfully.

5.8 Handling of unknown, unforeseen and erroneous protocol data

When a PDCP entity receives a PDCP PDU that contains reserved or invalid values, the PDCP entity shall:

- discard the received PDU.

6 Protocol data units, formats and parameters

6.1 Protocol data units

6.1.1 PDCP Data PDU

The PDCP Data PDU is used to convey:

- a PDCP SDU SN; and
- user plane data containing a PDCP SDU; or
- control plane data; and
- a MAC-I field for SRBs;

6.1.2 PDCP Control PDU

The PDCP Control PDU is used to convey:

- a PDCP status report indicating which PDCP SDUs are missing and which are not following a PDCP re-establishment.

6.2 Formats

6.2.1 General

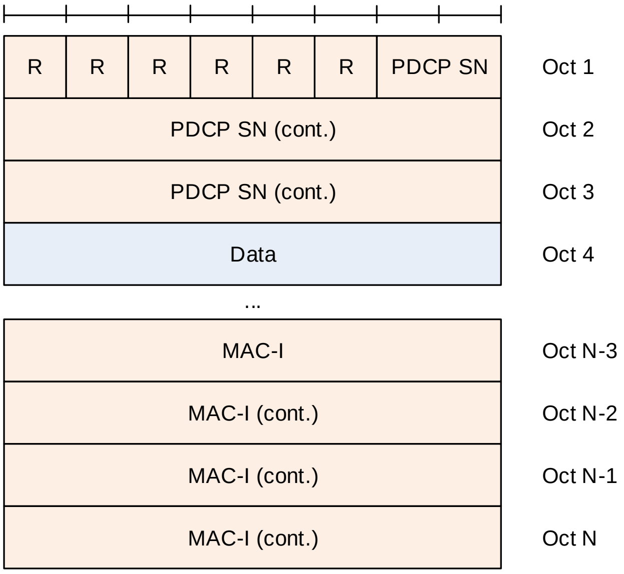
A PDCP PDU is a bit string that is byte aligned (i.e. multiple of 8 bits) in length. In the figures in sub clause 6.2, bit strings are represented by tables in which the most significant bit is the leftmost bit of the first line of the table, the least significant bit is the rightmost bit on the last line of the table, and more generally the bit string is to be read from left to right and then in the reading order of the lines. The bit order of each parameter field within a PDCP PDU is represented with the first and most significant bit in the leftmost bit and the last and least significant bit in the rightmost bit.

PDCP SDUs are bit strings that are byte aligned (i.e. multiple of 8 bits) in length. A SDU is included into a PDCP PDU from the first bit onward.

6.2.2 Control plane PDCP Data PDU

NOTE: It is applicable only in standalone mode

Figure 6.2.2.1 shows the format of the PDCP Data PDU carrying data for control plane SRBs.



R	R	R	R	R	R	PDCP SN	Oct 1
PDCP SN (cont.)							Oct 2
PDCP SN (cont.)							Oct 3
Data							Oct 4
...							
MAC-I							Oct N-3
MAC-I (cont.)							Oct N-2
MAC-I (cont.)							Oct N-1
MAC-I (cont.)							Oct N

Figure 6.2.2.1: PDCP Data PDU format for SRBs

6.2.6 PDCP Control PDU for PDCP status report

Figure 6.2.6.3 shows the format of the PDCP Control PDU carrying one PDCP status report when an 18 bit SN length is used. This format is applicable for DRBs mapped on RLC AM.

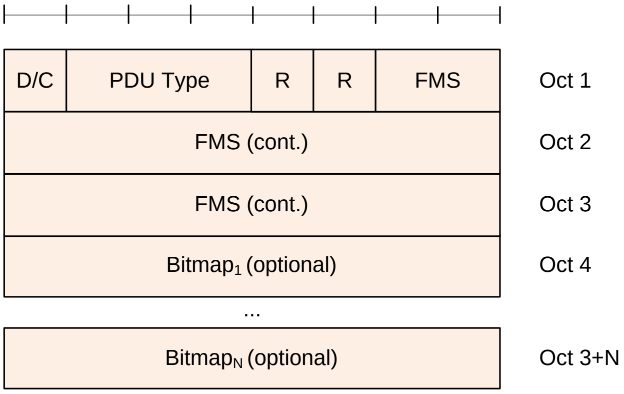


Figure 6.2.6.3: PDCP Control PDU format for PDCP status report using an 18 bit SN

6.2.7-10 Void

6.2.11 User plane PDCP Data PDU with PDCP SN (18 bits)

Figure 6.2.11.1 shows the format of the PDCP Data PDU when an 18 bit SN length is used. This format is applicable for PDCP Data PDUs carrying data from DRBs mapped on RLC AM or RLC UM..

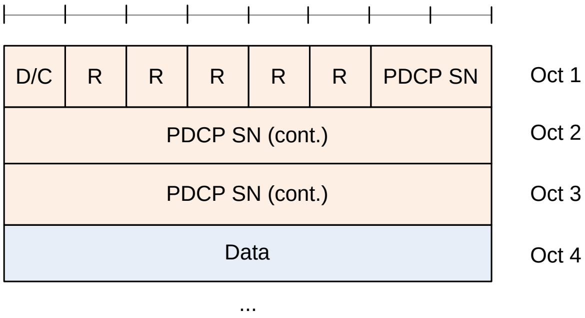


Figure 6.2.11.1: PDCP Data PDU format for DRBs using an 18 bit SN

6.3 Parameters

6.3.1 General

If not otherwise mentioned in the definition of each field then the bits in the parameters shall be interpreted as follows: the left most bit string is the first and most significant and the right most bit is the last and least significant bit.

Unless otherwise mentioned, integers are encoded in standard binary encoding for unsigned integers. In all cases the bits appear ordered from MSB to LSB when read in the PDU.

6.3.2 PDCP SN

Length: 18 bits as indicated in table 6.3.2.1.

Table 6.3.2.1: PDCP SN length

Length	Description
18	SRBs
18	DRBs

6.3.3 Data

Length: Variable

The Data field may include either one of the following:

- PDCP SDU (user plane data, or control plane data is valid only in standalone mode); -

6.3.4 MAC-I

NOTE: It is applicable only in standalone mode

Length: 32 bits

The MAC-I field carries a message authentication code calculated as specified in subclause 5.7.

For control plane data that are not integrity protected, the MAC-I field is still present and should be padded with padding bits set to 0.

6.3.5 COUNT

Length: 32 bits

For ciphering and integrity a COUNT value is maintained. The COUNT value is composed of a HFN and the PDCP SN. The length of the PDCP SN is configured by upper layers.

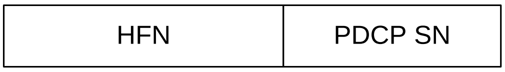


Figure 6.3.5.1: Format of COUNT

The size of the HFN part in bits is equal to 32 minus the length of the PDCP SN.

NOTE: When performing comparison of values related to COUNT, the UE takes into account that COUNT is a 32-bit value, which may wrap around (e.g., COUNT value of 2^{32} - 1 is less than COUNT value of 0).

6.3.6 R

Length: 1 bit

Reserved. In this version of the specification reserved bits shall be set to 0. Reserved bits shall be ignored by the receiver.

6.3.7 D/C

Length: 1 bit

Table 6.3.7.1: D/C field

Bit	Description
0	Control PDU
1	Data PDU

6.3.8 PDU type

Length: 3 bits

Table 6.3.8.1: PDU type

Bit	Description
000	PDCP status report
001-111	reserved

6.3.9 FMS

Length: 18 bits when an 18 bit SN length is used

PDCP SN of the first missing PDCP SDU.

6.3.10 Bitmap

Length: Variable

The length of the bitmap field can be 0.

The MSB of the first octet of the type "Bitmap" indicates whether or not the PDCP SDU with the SN (FMS + 1) modulo (Maximum_PDCP_SN + 1) has been received. The LSB of the first octet of the type "Bitmap" indicates whether or not the PDCP SDU with the SN (FMS + 8) modulo (Maximum_PDCP_SN + 1) has been received .

Table 6.3.10.1 Bitmap

Bit	Description
0	PDCP SDU with PDCP SN = (FMS + bit position) modulo (Maximum_PDCP_SN + 1) is missing in the receiver. The bit position of Nth bit in the Bitmap is N, i.e., the bit position of the first bit in the Bitmap is 1.
1	PDCP SDU with PDCP SN = (FMS + bit position) modulo (Maximum_PDCP_SN + 1) does not need to be retransmitted. The bit position of Nth bit in the Bitmap is N, i.e., the bit position of the first bit in the Bitmap is 1.

The UE fills the bitmap indicating which SDUs are missing (unset bit - ’0’), i.e. whether an SDU has not been received or, and which SDUs do not need retransmission (set bit - ’1’), i.e. whether an SDU has been received correctly.

7 Variables, constants and timers

7.1 State variables

This sub clause describes the state variables used in PDCP entities in order to specify the PDCP protocol.

All state variables are non-negative integers.

The transmitting side of each PDCP entity shall maintain the following state variables:

a) Next_PDCP_TX_SN

The variable Next_PDCP_TX_SN indicates the PDCP SN of the next PDCP SDU for a given PDCP entity. At establishment of the PDCP entity, the UE shall set Next_PDCP_TX_SN to 0.

b) TX_HFN

The variable TX_HFN indicates the HFN value for the generation of the COUNT value used for PDCP PDUs for a given PDCP entity. At establishment of the PDCP entity, the UE shall set TX_HFN to 0.

The receiving side of each PDCP entity shall maintain the following state variables:

c) Next_PDCP_RX_SN

The variable Next_PDCP_RX_SN indicates the next expected PDCP SN by the receiver for a given PDCP entity. At establishment of the PDCP entity, the UE shall set Next_PDCP_RX_SN to 0.

d) RX_HFN

The variable RX_HFN indicates the HFN value for the generation of the COUNT value used for the received PDCP PDUs for a given PDCP entity. At establishment of the PDCP entity, the UE shall set RX_HFN to 0.

e) Last_Submitted_PDCP_RX_SN

For PDCP entities for DRBs mapped on RLC AM the variable Last_Submitted_PDCP_RX_SN indicates the SN of the last PDCP SDU delivered to the upper layers. At establishment of the PDCP entity, the UE shall set Last_Submitted_PDCP_RX_SN to Maximum_PDCP_SN.

7.2 Timers

The transmitting side of each PDCP entity for DRBs shall maintain the following timers:

a) *discardTimer*

The duration of the timer is configured by upper layers [2]. In the transmitter, a new timer is started upon reception of an SDU from upper layer.

7.3 Constants

a) Reordering_Window

Indicates the size of the reordering window.131072 when 18 bit SN length is used, i.e. half of the PDCP SN space, for radio bearers that are mapped on RLC AM.

b) Maximum_PDCP_SN is:

- 262143 if the PDCP entity is configured for the use of 18 bits SNs

Annex A (informative): Change history

Change history after change control							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2016.04					First Skeleton and initial content		0.1.0
2016.06					Completion of v1.0.0	0.1.0	1.0.0