ETSI TS 136 323 V13.0.0 (2016-01)

TECHNICAL SPECIFICATION

LTE;
Evolved Universal Terrestrial Radio Access (E-UTRA);
Packet Data Convergence Protocol (PDCP) specification
(3GPP TS 36.323 version 13.0.0 Release 13)

Reference
RTS/TSGR-0236323vd00

Keywords
LTE

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document provides the description of the Packet Data Convergence Protocol (PDCP).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description".

[3] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol Specification".

[4] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA) Medium Access Control (MAC) protocol specification".

[5] 3GPP TS 36.322: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Link Control (RLC) protocol specification".

[6] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture".

[7] IETF RFC 4995: "The RObust Header Compression (ROHC) Framework".

[8] IETF RFC 4996: "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)".

[9] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed".

[10] IETF RFC 3843: "RObust Header Compression (ROHC): A Compression Profile for IP".

[11] IETF RFC 4815: "RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095".

[12] IETF RFC 5225: "RObust Header Compression (ROHC) Version 2: Profiles for RTP, UDP, IP, ESP and UDP Lite'.

[13] 3GPP TS 33.303: 'Proximity-based Services; Security Aspects'.

[14] 3GPP TS 23.303: 'Proximity-based Services; Stage 2'.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Split bearer: in dual connectivity, a bearer whose radio protocols are located in both the MeNB and the SeNB to use both MeNB and SeNB resources.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AM	Acknowledged Mode
ARP	Address Resolution Protocol
CID	Context Identifier
DRB	Data Radio Bearer carrying user plane data
EPS	Evolved Packet System
E-UTRA	Evolved UMTS Terrestrial Radio Access
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
eNB	E-UTRAN Node B
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
MCG	Master Cell Group
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PEK	ProSe Encryption Key
PGK	ProSe Group Key
ProSe	Proximity-based Services
PTK	ProSe Traffic Key
R	Reserved
RB	Radio Bearer
RFC	Request For Comments
RLC	Radio Link Control
RN	Relay Node
ROHC	RObust Header Compression
RRC	Radio Resource Control
RTP	Real Time Protocol
SAP	Service Access Point
SCG	Secondary Cell Group
SDU	Service Data Unit
SLRB	Sidelink Radio Bearer carrying Sidelink Communication data
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. Functionality specified for the UE equally applies to the RN for functionality necessary for the RN. There is also functionality which is only applicable to the RN in its communication with the E-UTRAN, in which case the specification denotes the RN instead of the UE. RN-specific behaviour is not applicable to the UE. The functionality specified for the UE applies to communication on Uu interface and PC5 interface [14].

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 [2].

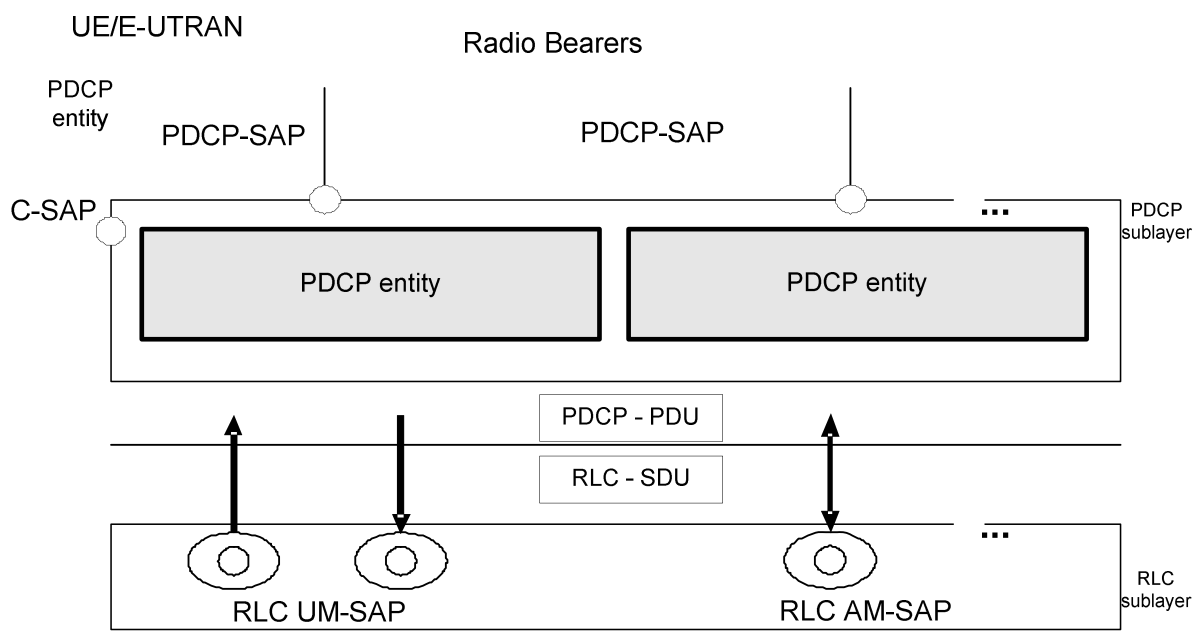

Figure 4.2.1.1 - PDCP layer, structure view

Each RB (i.e. DRB, SLRB 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 the RB characteristic (i.e. uni-directional or bi-directional) and RLC mode. For split bearers, each PDCP entity is associated with two AM RLC entities. The PDCP entities are located in the PDCP sublayer.

The PDCP sublayer is configured by upper layers [3].

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 carrying user plane data may be configured to use header compression.

Each PDCP entity is carrying the data of one radio bearer. In this version of the specification, only the robust header compression protocol (ROHC), is supported. Every PDCP entity uses at most one ROHC compressor instance and at most one ROHC decompressor instance.

A PDCP entity is associated either to the control plane or the user plane depending on which radio bearer it is carrying data for.

Figure 4.2.2.1 represents the functional view of the PDCP entity for the PDCP sublayer; it should not restrict implementation. The figure is based on the radio interface protocol architecture defined in [2].

For RNs, integrity protection and verification are also performed for the u-plane.

For split bearers, routing is performed in the transmitting PDCP entity, and reordering is performed in the receiving PDCP entity. When submitting PDCP PDUs to lower layers upon request from lower layers, the transmitting PDCP entity shall:

- if *ul-Data SplitThreshold* is configured and the data available for transmission is larger than or equal to *ul-Data SplitThreshold*:
  - submit the PDCP PDUs to either the associated AM RLC entity configured for SCG or the associated AM RLC entity configured for MCG;
- else:
  - if *ul-DataSplitDRB-ViaSCG* is set to *TRUE* by upper layers [3]:
    - submit the PDCP PDUs to the associated AM RLC entity configured for SCG;
  - else:
    - submit the PDCP PDUs to the associated AM RLC entity configured for MCG.

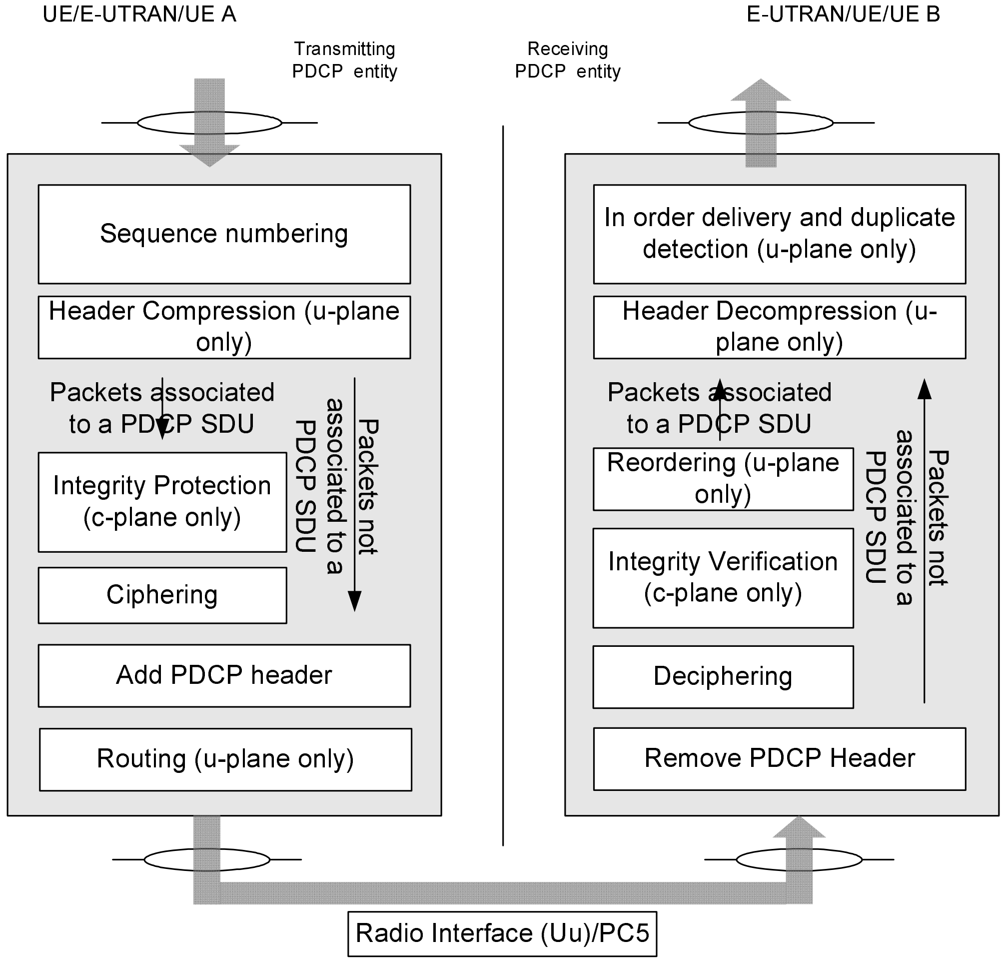

Figure 4.2.2.1 - PDCP layer, functional view

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 or to the relay at the evolved Node B (eNB). The following services are provided by PDCP to upper layers:

- transfer of user plane data;
- transfer of control plane data;
- header compression;
- ciphering;
- integrity protection.

The maximum supported size of a PDCP SDU is 8188 octets. The maximum supported size of a PDCP Control PDU is 8188 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 [5]):

- 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:

- header compression and decompression of IP data flows using the ROHC protocol;
- transfer of data (user plane or control plane);
- 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;
- integrity protection and integrity verification of control plane data;
- for RNs, integrity protection and integrity verification of user plane data;
- timer based discard;
- duplicate discarding;
- for split bearers, routing and reordering.

PDCP uses the services provided by the RLC sublayer.

PDCP is used for SRBs, DRBs, and SLRBs mapped on DCCH, DTCH, and STCH 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.

For split bearers, when indicating the data available for transmission to the MAC entity for BSR triggering and Buffer Size calculation, the UE shall:

- if *ul-Data SplitThreshold* is configured and the data available for transmission is larger than or equal to *ul-Data SplitThreshold*:
  - indicate the data available for transmission to both the MAC entity configured for SCG and the MAC entity configured for MCG;
- else:
  - if *ul-DataSplitDRB-ViaSCG* is set to *TRUE* by upper layer [3]:
    - indicate the data available for transmission to the MAC entity configured for SCG only;
    - if *ul-Data SplitThreshold* is configured, indicate the data available for transmission as 0 to the MAC entity configured for MCG;
  - else:
    - indicate the data available for transmission to the MAC entity configured for MCG only;
    - if *ul-DataSplitThreshold* is configured, indicate the data available for transmission as 0 to the MAC entity configured for SCG.

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 header compression of the PDCP SDU (if configured) as specified in the subclause 5.5.4;
- 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 when the reordering function is not used

For DRBs mapped on RLC AM, when the reordering function is not used, 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;
  - perform header decompression (if configured) as specified in the subclause 5.5.5;
  - 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 and header decompression (if configured) for the PDCP PDU as specified in the subclauses 5.6 and 5.5.5, respectively;
  - 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.

5.1.2.1.2a RN procedures for DRBs mapped on RLC AM

For DRBs mapped on RLC AM, at reception of a PDCP Data PDU from lower layers, the RN should follow the procedures specified for a UE in 5.1.2.1.2 with the addition that for DRBs for which integrity verification is configured, the RN should, immediately after performing deciphering as specified in 5.6, also perform integrity verification as specified in 5.7 with the same COUNT value as used for deciphering.

In case of integrity verification failure, the RN should discard the PDCP Data PDU without performing header decompression and without delivering any stored PDCP SDU(s) to upper layers. The RN should also set the RX_HFN, Next_PDCP_RX_SN and Last_Submitted_PDCP_RX_SN to the respective values they had before the reception of the PDCP Data PDU.

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;
- perform header decompression (if configured) of the deciphered PDCP Data PDU as specified in the subclause 5.5.5;
- deliver the resulting PDCP SDU to upper layer.

5.1.2.1.3a RN procedures for DRBs mapped on RLC UM

For DRBs mapped on RLC UM, at reception of a PDCP Data PDU from lower layers, the RN should follow the procedures specified for a UE in 5.1.2.1.3 with the addition that for DRBs for which integrity verification is configured, the RN should, immediately after performing deciphering as specified in 5.6, also perform integrity verification as specified in 5.7 with the same COUNT value as used for deciphering.

In case of integrity verification failure, the RN should discard the PDCP Data PDU without performing header decompression and set the RX_HFN and Next_PDCP_RX_SN to the respective values they had before the reception of the PDCP Data PDU.

5.1.2.1.4 Procedures for DRBs mapped on RLC AM when the reordering function is used

For DRBs mapped on RLC AM, the PDCP entity shall use the reordering function as specified in this section when:

- the PDCP entity is associated with two AM RLC entities; or
- the PDCP entity is associated with one AM RLC entity after it was, according to the most recent reconfiguration, associated with two AM RLC entities without performing PDCP re-establishment.

The PDCP entity shall not use the reordering function in other cases.

5.1.2.1.4.1 Procedures when a PDCP PDU is received from the lower layers

For DRBs mapped on RLC AM, when there ordering function is used, 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:
  - discard the PDCP PDU;
- 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:
  - if a PDCP SDU with the same PDCP SN is stored:
    - discard the PDCP PDU;
  - else:

        - perform deciphering of the PDCP PDU and store the resulting PDCP SDU;
    - 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 PDU;
        - set Last_Submitted_PDCP_RX_SN to the PDCP SN of the last PDCP SDU delivered to upper layers;
    - if *t-Reordering* is running:
        - if the PDCP SDU with Reordering_PDCP_RX_COUNT – 1 has been delivered to upper layers:
            - stop and reset *t-Reordering*;
    - if *t-Reordering* is not running (includes the case when *t-Reordering* is stopped due to actions above):
        - if there is at least one stored PDCP SDU:
            - start *t-Reordering*;
            - set Reordering_PDCP_RX_COUNT to the COUNT value associated to RX_HFN and Next_PDCP_RX_SN.

5.1.2.1.4.2 Procedures when *t-Reordering* expires

When *t-Reordering* expires, the UE shall:

- deliver to upper layers in ascending order of the associated COUNT value:
    - all stored PDCP SDU(s) with associated COUNT value(s) less than Reordering_PDCP_RX_COUNT;
    - all stored PDCP SDU(s) with consecutively associated COUNT value(s) starting from Reordering_PDCP_RX_COUNT;
- set Last_Submitted_PDCP_RX_SN to the PDCP SN of the last PDCP SDU delivered to upper layers;
- if there is at least one stored PDCP SDU:
    - start *t-Reordering*;
    - set Reordering_PDCP_RX_COUNT to the COUNT value associated to RX_HFN and Next_PDCP_RX_SN.

5.1.2.1.4.3 Procedures when the value of *t-Reordering* is reconfigured

When the value of the *t-Reordering* is reconfigured by upper layers while the *t-Reordering* is running, the UE shall:

- stop and restart *t-Reordering*;
- set Reordering_PDCP_RX_COUNT to the COUNT value associated to RX_HFN and Next_PDCP_RX_SN.

5.1.2.2 Procedures for SRBs

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.

5.1.3 SL Data Transmission Procedures

For Sidelink transmission, the UE shall follow the procedures in subclause 5.1.1 with following modifications:

- the requirements for maintaining Next_PDCP_TX_SN and TX_HFN are not applicable;
- determine a PDCP SN ensuring that a PDCP SN value is not reused with the same key;
- perform ciphering (if configured) as specified in subclause 5.6.1;
- perform the header compression (if configured) if SDU Type is set to 000, i.e. IP SDUs.

5.1.4 SL Data Reception Procedures

For Sidelink reception, the UE shall follow the procedures in subclause 5.1.2.1.3 with following modifications:

- the requirements for maintaining Next_PDCP_RX_SN and RX_HFN are not applicable;
- perform the deciphering (if configured) as specified in subclause 5.6.1;
- perform the header decompression (if configured) if SDU Type is set to 000, i.e. IP SDUs.

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:

- reset the header compression protocol for uplink and start with an IR state in U-mode (if configured) [9] [11];

- if connected as an RN, apply the integrity protection algorithm and key provided by upper layers (if configured) during the re-establishment procedure;
- 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 header compression of the PDCP SDU (if configured) as specified in the subclause 5.5.4;
    - if connected as an RN, perform integrity protection (if configured) of the PDCP SDU using the COUNT value associated with this PDCP SDU as specified in the subclause 5.7;
    - 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:

- reset the header compression protocol for uplink and start with an IR state in U-mode [9] [11] if the DRB is configured with the header compression protocol and *drb-ContinueROHC* is not configured [3];
- 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;
- if connected as an RN, apply the integrity protection algorithm and key provided by upper layers (if configured) 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

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 while the reordering function is not used

When upper layers request a PDCP re-establishment while the reordering function is not used, 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;

- reset the header compression protocol for downlink and start with NC state in U-mode (if configured) [9] [11];
- apply the ciphering algorithm and key provided by upper layers during the re-establishment procedure.
- if connected as an RN, apply the integrity protection algorithm and key provided by upper layers (if configured) during the re-establishment procedure.

5.2.2.1a Procedures for DRBs mapped on RLC AM while the reordering function is used

When upper layers request a PDCP re-establishment while the reordering function is used, the UE shall:

- process the PDCP Data PDU(s) that are received from lower layers due to the re-establishment of the lower layers, as specified in the subclause 5.1.2.1.4;
- if the PDCP entity is to be associated with one AM RLC entity after PDCP re-establishment:
    - stop and reset *t-Reordering*;
- 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;
- reset the header compression protocol for downlink and start with NC state in U-mode [9] [11] if the DRB is configured with the header compression protocol and *drb-ContinueROHC* is not configured [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.
- if connected as an RN, apply the integrity protection algorithm and key provided by upper layers (if configured) during the re-establishment procedure.

5.2.2.3 Procedures for SRBs

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* [3]), 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 8188 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, and optionally PDCP SDUs for which decompression have failed;
- 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.

NOTE: For UL split bearers, discarding a PDCP SDU already associated with a PDCP SN causes a SN gap in the transmitted PDCP PDUs, which increases PDCP reordering delay in the receiving PDCP entity. It is up to UE implementation how to minimize SN gap after SDU discard.

5.5 Header Compression and Decompression

5.5.1 Supported header compression protocols and profiles

The header compression protocol is based on the Robust Header Compression (ROHC) framework [7]. There are multiple header compression algorithms, called profiles, defined for the ROHC framework. Each profile is specific to the particular network layer, transport layer or upper layer protocol combination e.g. TCP/IP and RTP/UDP/IP.

The detailed definition of the ROHC channel is specified as part of the ROHC framework in RFC 4995 [7]. This includes how to multiplex different flows (header compressed or not) over the ROHC channel, as well as how to associate a specific IP flow with a specific context state during initialization of the compression algorithm for that flow.

The implementation of the functionality of the ROHC framework and of the functionality of the supported header compression profiles is not covered in this specification.

In this version of the specification the support of the following profiles is described:

Table 5.5.1.1: Supported header compression protocols and profiles

Profile Identifier	Usage:	Reference
0x0000	No compression	RFC 4995
0x0001	RTP/UDP/IP	RFC 3095, RFC 4815
0x0002	UDP/IP	RFC 3095, RFC 4815
0x0003	ESP/IP	RFC 3095, RFC 4815
0x0004	IP	RFC 3843, RFC 4815
0x0006	TCP/IP	RFC 4996
0x0101	RTP/UDP/IP	RFC 5225
0x0102	UDP/IP	RFC 5225
0x0103	ESP/IP	RFC 5225
0x0104	IP	RFC 5225

5.5.2 Configuration of header compression

PDCP entities associated with DRBs can be configured by upper layers [3] to use header compression. PDCP entities associated with SLRBs can be configured to use header compression for IP SDUs.

5.5.3 Protocol parameters

RFC 4995 has configuration parameters that are mandatory and that must be configured by upper layers between compressor and decompressor peers [7]; these parameters define the ROHC channel. The ROHC channel is a unidirectional channel, i.e. there is one channel for the downlink, and one for the uplink. There is thus one set of parameters for each channel, and the same values shall be used for both channels belonging to the same PDCP entity.

These parameters are categorized in two different groups, as defined below:

- M: Mandatory and configured by upper layers.
- N/A: Not used in this specification.

The usage and definition of the parameters shall be as specified below.

- MAX_CID (M): This is the maximum CID value that can be used. One CID value shall always be reserved for uncompressed flows. The parameter MAX_CID is configured by upper layers (*maxCID* [3]).
- LARGE_CIDS: This value is not configured by upper layers, but rather it is inferred from the configured value of MAX_CID according to the following rule:

  If MAX_CID > 15 then LARGE_CIDS = TRUE else LARGE_CIDS = FALSE.

- PROFILES (M): Profiles are used to define which profiles are allowed to be used by the UE. The list of supported profiles is described in section 5.5.1. The parameter PROFILES is configured by upper layers (*profiles* [3]).
- FEEDBACK_FOR (N/A): This is a reference to the channel in the opposite direction between two compression endpoints and indicates to what channel any feedback sent refers to. Feedback received on one ROHC channel for this PDCP entity shall always refer to the ROHC channel in the opposite direction for this same PDCP entity.
- MRRU (N/A): ROHC segmentation is not used.

5.5.4 Header compression

The header compression protocol generates two types of output packets:

- compressed packets, each associated with one PDCP SDU
- standalone packets not associated with a PDCP SDU, i.e. interspersed ROHC feedback packets

A compressed packet is associated with the same PDCP SN and COUNT value as the related PDCP SDU.

Interspersed ROHC feedback packets are not associated with a PDCP SDU. They are not associated with a PDCP SN and are not ciphered.

NOTE: If the MAX_CID number of ROHC contexts are already established for the compressed flows and a new IP flow does not match any established ROHC context, the compressor should associate the new IP flow with one of the ROHC CIDs allocated for the existing compressed flows or send PDCP SDUs belonging to the IP flow as uncompressed packet.

5.5.5 Header decompression

If header compression is configured by upper layers for PDCP entities associated with u-plane data the PDCP PDUs are de-compressed by the header compression protocol after performing deciphering as explained in the subclause 5.6.

5.5.6 PDCP Control PDU for interspersed ROHC feedback packet

5.5.6.1 Transmit Operation

When an interspersed ROHC feedback packet is generated by the header compression protocol, the UE shall:

- submit to lower layers the corresponding PDCP Control PDU as specified in subclause 6.2.5 i.e. without associating a PDCP SN, nor performing ciphering.

5.5.6.2 Receive Operation

At reception of a PDCP Control PDU for interspersed ROHC feedback packet from lower layers, the UE shall:

- deliver the corresponding interspersed ROHC feedback packet to the header compression protocol without performing deciphering.

5.6 Ciphering and Deciphering

The ciphering function includes both ciphering and deciphering and is performed in PDCP. For the control plane, 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.

For RNs, for the user plane, in addition to the data part of the PDCP PDU, the MAC-I (see 6.3.4) is also ciphered if integrity protection is configured.

The ciphering algorithm and key to be used by the PDCP entity are configured by upper layers [3] and the ciphering method shall be applied as specified in [6].

The ciphering function is activated by upper layers [3]. After security activation, the ciphering function shall be applied to all PDCP PDUs indicated by upper layers [3] 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 [6] 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 [6]).The parameters required by PDCP which are provided by upper layers [3] are listed below:

- BEARER (defined as the radio bearer identifier in [6]. It will use the value RB identity –1 as in [3]);

- KEY (the ciphering keys for the control plane and for the user plane are K_{RRCenc} and K_{UPenc}, respectively).

5.6.1 SL Ciphering and Deciphering for one-to-many communication

For SLRB used for one-to-many communication, the ciphering function includes both ciphering and deciphering and is performed in PDCP as defined in [13]. The data unit that is ciphered is the data part of the PDCP PDU (see subclause 6.3.3). The ciphering function as specified in [6] is applied with KEY (PEK), COUNT (derived from PTK Identity and PDCP SN as specified in [13]), BEARER and DIRECTION (set to 0) as input. The ciphering function is configured by ProSe Function.

If ciphering is configured, the ciphering algorithm and related parameters including PGK, PGK Identity, and Group Member Identity are configured to the UE by ProSe Key Management Function. The UE shall set PTK Identity based on PGK, PGK Identity, and PDCP SN as specified in [13]. The UE shall derive PTK from PGK using PTK Identity and Group Member Identity, and derive PEK from PTK using the ciphering algorithm. The PGK Index, PTK Identity, and PDCP SN are included in the PDCP PDU header.

If ciphering is not configured, PGK Index, PTK Identity, and PDCP SN shall be set to '0' in the PDCP PDU header.

5.6.2 SL Ciphering and Deciphering for one-to-one communication

For SLRB used for one-to-one communication, the ciphering function includes both ciphering and deciphering and is performed in PDCP of SLRB that needs ciphering and deciphering as defined in [13]. The data unit that is ciphered is the data part of the PDCP PDU (see subclause 6.3.3). The ciphering function as specified in [6] is applied with KEY (PEK), COUNT (derived from $K_{D\text{-}sess}$ Identity and PDCP SN as specified in [13]), BEARER and DIRECTION (which value shall be set is specified in [13]) as input.

For the SLRB that needs ciphering and deciphering, the UE shall derive the KEY (PEK) based on $K_{D\text{-}sess}$ and the algorithms determined by the initiating UE and the receiving UE as specified in [13]. The $K_{D\text{-}sess}$ Identity and PDCP SN are included in the PDCP PDU header.

For the SLRB that does not need ciphering and deciphering, the UE shall set $K_{D\text{-}sess}$ and PDCP SN to '0' in the PDCP PDU header.

5.7 Integrity Protection and Verification

The integrity protection function includes both integrity protection and integrity verification and is performed in PDCP for PDCP entities associated with SRBs and the SLRB that needs integrity protection. The data unit that is integrity protected is the PDU header and the data part of the PDU before ciphering.

For RNs, the integrity protection function is performed also for PDCP entities associated with DRBs if integrity protection is configured.

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 [6].

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 [6] 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 [6]). The parameters required by PDCP which are provided by upper layers [3] are listed below:

- BEARER (defined as the radio bearer identifier in [6]. It will use the value RB identity –1 as in [3]);
- KEY (K_{RRCint}).

- for RNs, KEY (K_{UPint})

For the SLRB that needs integrity protection and verification, the parameters that are required by PDCP for integrity protection are defined in [6] and are input to the integrity protection algorithm. The required inputs to the integrity protection function include the COUNT value and DIRECTION (which value shall be set is specified in [13]). The parameters required by PDCP which are provided by upper layers [3] are listed below:

- BEARER (defined as the radio bearer identifier in [6]);
- KEY (PIK).

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.

5.9 PDCP Data Recovery procedure

When upper layers request a PDCP Data Recovery for a radio bearer, the UE shall:

- if the radio bearer is configured by upper layers to send a PDCP status report in the uplink (*statusReportRequired* [3]), compile a status report as described in subclause 5.3.1, and submit it to lower layers as the first PDCP PDU for the transmission;
- perform retransmission of all the PDCP PDUs previously submitted to re-established AM RLC entity in ascending order of the associated COUNT values from the first PDCP PDU for which the successful delivery has not been confirmed by lower layers.

After performing the above procedures, the UE shall follow the procedures in subclause 5.1.1.

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
- for SLRBs used for one-to-many communication, PGK Index, PTK Identity, and SDU type; or
- for SLRBs used for one-to-one communication, $K_{D\text{-}sess}$ Identity, and SDU type; and
- user plane data containing an uncompressed PDCP SDU; or
- user plane data containing a compressed PDCP SDU; or
- control plane data; and
- a MAC-I field for SRBs; or
- for the SLRB that needs integrity protection for one-to-one communication, a MAC-I field; or

- for RNs, a MAC-I field for DRB (if integrity protection is configured);

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.
- header compression control information, e.g. interspersed ROHC feedback.

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 compressed or uncompressed SDU is included into a PDCP PDU from the first bit onward.

6.2.2 Control plane PDCP Data PDU

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

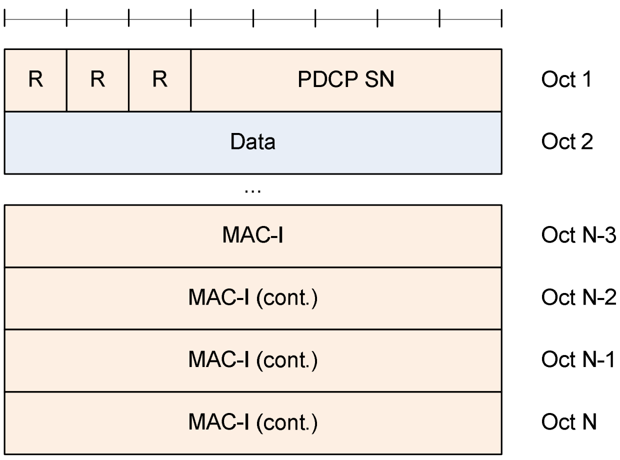

Figure 6.2.2.1: PDCP Data PDU format for SRBs

6.2.3 User plane PDCP Data PDU with long PDCP SN (12 bits)

Figure 6.2.3.1 shows the format of the PDCP Data PDU when a 12 bit SN length is used. This format is applicable for PDCP Data PDUs carrying data from DRBs mapped on RLC AM or RLC UM.

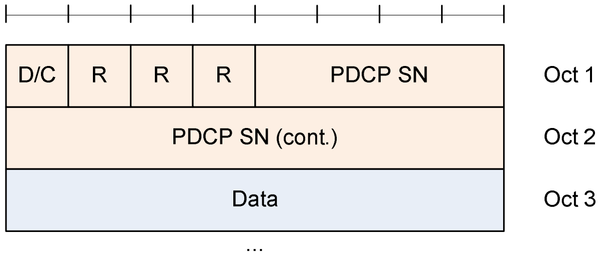

Figure 6.2.3.1: PDCP Data PDU format for DRBs using a 12 bit SN

6.2.4 User plane PDCP Data PDU with short PDCP SN (7 bits)

Figure 6.2.4.1 shows the format of the PDCP Data PDU when a 7 bit SN length is used. This format is applicable for PDCP Data PDUs carrying data from DRBs mapped on RLC UM.

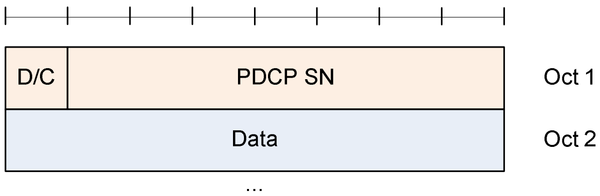

Figure 6.2.4.1: PDCP Data PDU format for DRBs using 7 bit SN

6.2.5 PDCP Control PDU for interspersed ROHC feedback packet

Figure 6.2.5.1 shows the format of the PDCP Control PDU carrying one interspersed ROHC feedback packet. This format is applicable for DRBs mapped on RLC AM or RLC UM.

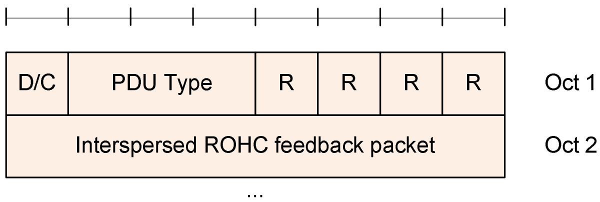

Figure 6.2.5.1: PDCP Control PDU format for interspersed ROHC feedback packet

6.2.6 PDCP Control PDU for PDCP status report

Figure 6.2.6.1 shows the format of the PDCP Control PDU carrying one PDCP status report when a 12 bit SN length is used, Figure 6.2.6.2 shows the format of the PDCP Control PDU carrying one PDCP status report when a 15 bit SN length is used, and 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.

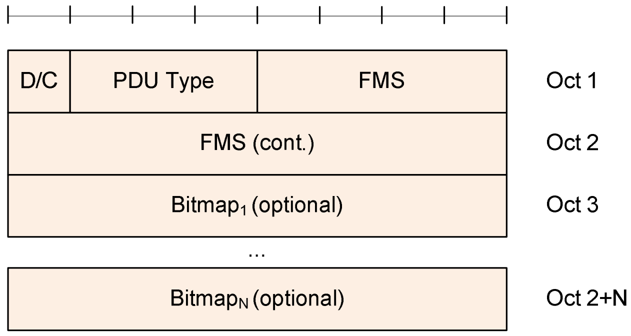

Figure 6.2.6.1: PDCP Control PDU format for PDCP status report using a 12 bit SN

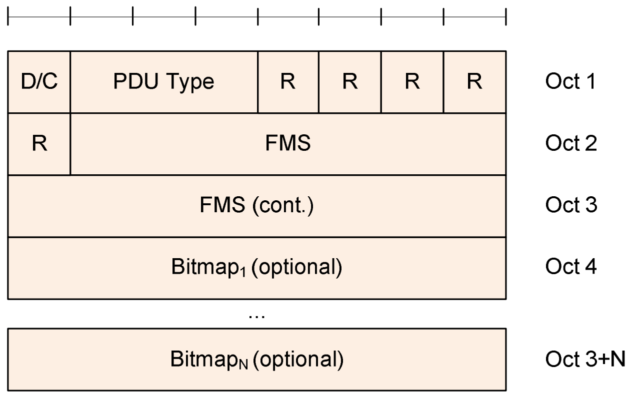

Figure 6.2.6.2: PDCP Control PDU format for PDCP status report using a 15 bit SN

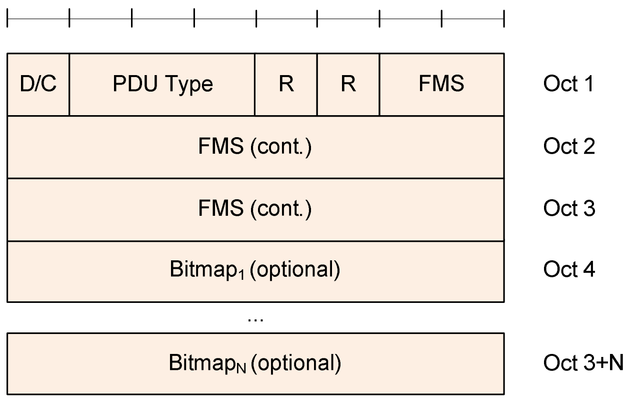

Figure 6.2.6.3: PDCP Control PDU format for PDCP status report using an 18 bit SN

6.2.7 Void

6.2.8 RN user plane PDCP Data PDU with integrity protection

Figure 6.2.8.1 shows the format of the PDCP Data PDU for RNs when integrity protection is used. This format is applicable for PDCP Data PDUs carrying data from DRBs mapped on RLC AM or RLC UM.

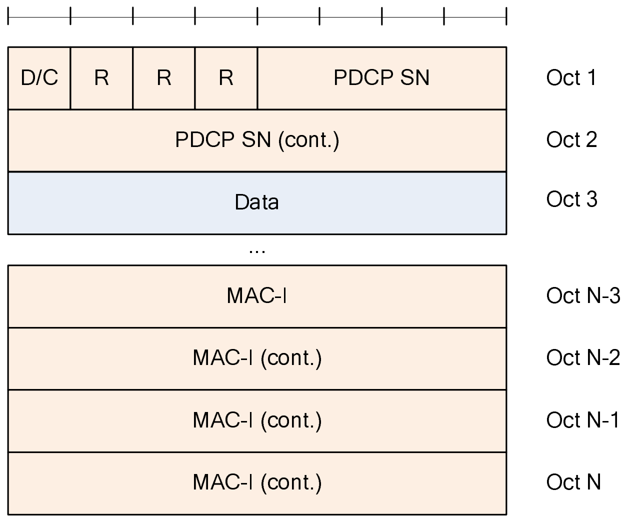

Figure 6.2.8.1: PDCP Data PDU format for RN DRBs using integrity protection

6.2.9 User plane PDCP Data PDU with extended PDCP SN (15 bits)

Figure 6.2.9.1 shows the format of the PDCP Data PDU when a 15 bit SN length is used. This format is applicable for PDCP Data PDUs carrying data from DRBs mapped on RLC AM.

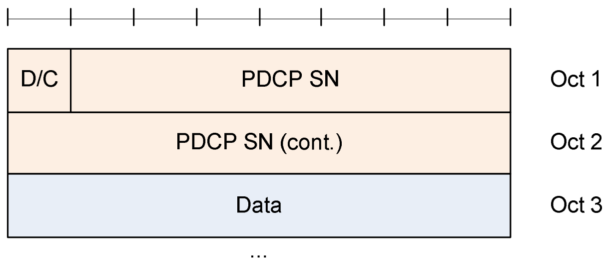

Figure 6.2.9.1: PDCP Data PDU format for DRBs using a 15 bit SN

6.2.10 User plane PDCP Data PDU for SLRB

Figure 6.2.10.1 shows the format of the PDCP Data PDU for SLRB used for one-to-many communication where a 16 bit SN length is used.

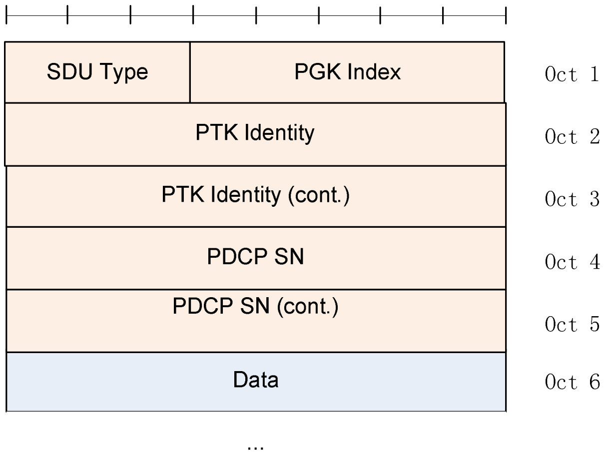

Figure 6.2.10.1: PDCP Data PDU format for SLRB used for one-to-many communication

Figure 6.2.10.2 shows the format of the PDCP Data PDU for SLRB used for one-to-one communication where a 16 bit SN length is used. MAC-I field is used only for the SLRB that needs integrity protection.

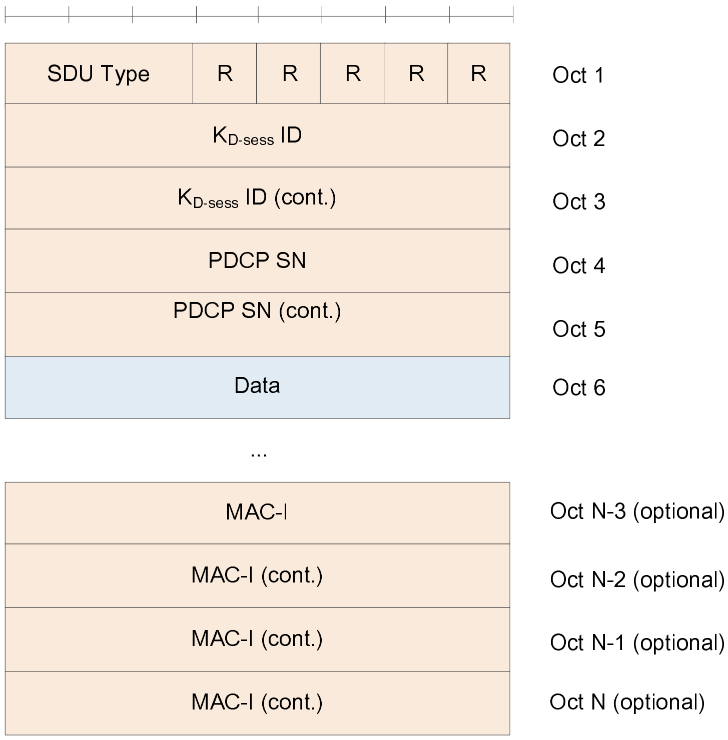

Figure 6.2.10.2: PDCP Data PDU format for SLRB used for one-to-one communication

6.2.11 User plane PDCP Data PDU with further extended 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.

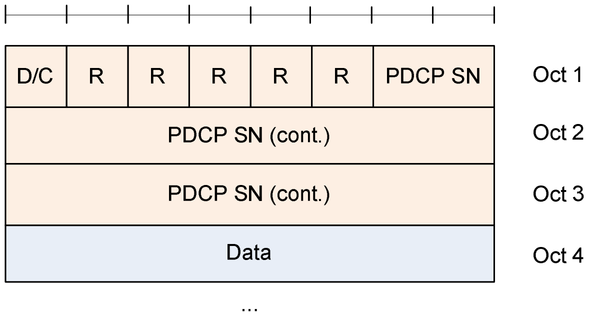

Figure 6.2.11.1: PDCP Data PDU format for DRBs using an 18 bit SN

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: 5, 7, 12, 15, 16, or 18 bits as indicated in table 6.3.2.1.

Table 6.3.2.1: PDCP SN length

Length	Description
5	SRBs
7	DRBs, if configured by upper layers (*pdcp-SN-Size* [3])
12	DRBs, if configured by upper layers (*pdcp-SN-Size* [3])
15	DRBs, if configured by upper layers (*pdcp-SN-Size* [3])
16	SLRBs
18	DRBs, if configured by upper layers (*pdcp-SN-Size* [3])

6.3.3 Data

Length: Variable

The Data field may include either one of the following:

- Uncompressed PDCP SDU (user plane data, or control plane data); or
- Compressed PDCP SDU (user plane data only).

6.3.4 MAC-I

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.

HFN	PDCP SN

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	Interspersed ROHC feedback packet
010-111	reserved

6.3.9 FMS

Length: 12 bits when a 12 bit SN length is used, 15 bits when a 15 bit SN length is used, and 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 and, optionally decompressed correctly. 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 and, optionally decompressed correctly.

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 N^{th} 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 N^{th} 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 optionally has been received but has not been decompressed correctly, and which SDUs do not need retransmission (set bit - "1"), i.e. whether an SDU has been received correctly and may or may not have been decompressed correctly.

6.3.11 Interspersed ROHC feedback packet

Length: Variable

Contains one ROHC packet with only feedback, i.e. a ROHC packet that is not associated with a PDCP SDU as defined in subclause 5.5.4.

6.3.12 PGK Index

Length: 5 bits

5 LSBs of PGK Identity as specified in [13].

6.3.13 PTK Identity

Length: 16 bits

PTK Identity as specified in [13].

6.3.14 SDU Type

Length: 3 bits

PDCP SDU type, i.e. Layer-3 Protocol Data Unit type as specified in [14]. PDCP entity may handle the SDU differently per SDU Type, e.g. header compression is applicable to IP SDU but not ARP SDU.

Table 6.3.14.1: SDU Type

Bit	Description
000	IP
001	ARP
010	PC5 Signaling
011-111	reserved

6.3.15 $K_{D\text{-}sess}$ ID

Length: 16 bits

$K_{D\text{-}sess}$ Identity as specified in [13].

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.

f) Reordering_PDCP_RX_COUNT

This variable is used only when the reordering function is used. This variable holds the value of the COUNT following the COUNT value associated with the PDCP PDU which triggered *t-Reordering*.

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 [3]. In the transmitter, a new timer is started upon reception of an SDU from upper layer.

The receiving side of each PDCP entity shall maintain the following timers only when the reordering function is used:

b) *t-Reordering*

The duration of the timer is configured by upper layers [3]. This timer is used to detect loss of PDCP PDUs as specified in the subclause 5.1.2.1.4. If *t-Reordering* is running, *t-Reordering* shall not be started additionally, i.e. only one *t-Reordering* per PDCP entity is running at a given time.

7.3 Constants

a) Reordering_Window

Indicates the size of the reordering window. The size equals to 2048 when a 12 bit SN length is used, 16384 when a 15 bit SN length is used, or 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
- 65535 if the PDCP entity is configured for the use of 16 bits SNs
- 32767 if the PDCP entity is configured for the use of 15 bits SNs
- 4095 if the PDCP entity is configured for the use of 12 bit SNs
- 127 if the PDCP entity is configured for the use of 7 bit SNs
- 31 if the PDCP entity is configured for the use of 5 bit SNs

Annex A (informative): Change history

Change history after change control							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2007-12	RP-38	RP-070919	-	-	Approved at TSG-RAN #38 and placed under Change Control	2.0.0	8.0.0
2008-03	RP-39	RP-080197	0001	-	CR to 36.323 with Update of E-UTRAN PDCP specification	8.0.0	8.1.0
2008-05	RP-40	RP-080412	0002	-	Clarification of the BSR calculation	8.1.0	8.2.0
	RP-40	RP-080412	0003	1	PDCP minor changes	8.1.0	8.2.0
	RP-40	RP-080387	0004	3	Addition of a duplicate discard window	8.1.0	8.2.0
	RP-40	RP-080412	0006	-	Reference to ROHCv2 profiles	8.1.0	8.2.0
	RP-40	RP-080412	0010	-	Bitmap in the DL PDCP status report	8.1.0	8.2.0
	-	-	-	-	Corrections to sections 5.5.1.1, 5.5.1.2.1 and 5.8 to correctly implement CR0004 Rev 3 (instead of CR0004 Rev 2 of RP-080412).	8.2.0	8.2.1
2008-09	RP-41	RP-080692	0013	-	Restructuring of PDCP specification	8.2.1	8.3.0
	RP-41	RP-080692	0016	-	Miscellaneous PDCP corrections	8.2.1	8.3.0
	RP-41	RP-080692	0023	-	Correction to the PDCP structure	8.2.1	8.3.0
	RP-41	RP-080692	0033	-	Initial TX_HFN and RX_HFN values	8.2.1	8.3.0
2008-12	RP-42	RP-081020	0038	-	Clarification with regards to the PDCP state variables	8.3.0	8.4.0
	RP-42	RP-081020	0039	-	CR 0039 to 36.323 on Correction to PDCP functional view	8.3.0	8.4.0
	RP-42	RP-081020	0040	-	PDCP 'in-sequence delivery and duplicate elimination' always on	8.3.0	8.4.0
	RP-42	RP-081020	0041	-	Proposed CR to 36.323 on Processing of PDCP SDU received from upper layer	8.3.0	8.4.0
	RP-42	RP-081020	0042	-	Error in AM receive window behaviour	8.3.0	8.4.0
	RP-42	RP-081020	0047	-	Proposed CR on the described scope of Last_Submitted_PDCP_RX_SN	8.3.0	8.4.0
	RP-42	RP-081020	0048	-	Proposed CR to move DIRECTION from parameters provided by upper layer	8.3.0	8.4.0
	RP-42	RP-081020	0049	-	Clarification on COUNT	8.3.0	8.4.0
	RP-42	RP-081020	0050	-	Correction to PDCP procedure for SRB	8.3.0	8.4.0
	RP-42	RP-081020	0052	-	Correction to the PDCP re-establishment procedure	8.3.0	8.4.0
	RP-42	RP-081020	0054	-	Correction to PDCP functional view	8.3.0	8.4.0
	RP-42	RP-081020	0055	-	Miscellaneous PDCP corrections	8.3.0	8.4.0
	RP-42	RP-081020	0057	-	Proposed CR for error handling	8.3.0	8.4.0
	RP-42	RP-081020	0060	-	Proposed CR to 36.323 on Correction to PDCP Control PDU description	8.3.0	8.4.0
	RP-42	RP-081020	0061	1	Corrections to PDCP STATUS REPORT	8.3.0	8.4.0
2009-03	RP-43	RP-090130	0064	-	CR to specify maximum PDCP SDU size	8.4.0	8.5.0
	RP-43	RP-090130	0065	-	CR with correction on PDCP function of maintaining SNs	8.4.0	8.5.0
	RP-43	RP-090130	0066	-	Miscellaneous corrections to 36.323	8.4.0	8.5.0
	RP-43	RP-090130	0067	-	Minor issues on PDCP	8.4.0	8.5.0
	RP-43	RP-090130	0068	-	Security related corrections	8.4.0	8.5.0
	RP-43	RP-090130	0069	-	CR to 36.323 on RRC Parameters	8.4.0	8.5.0
	RP-43	RP-090130	0070	1	Corrections on BSR reporting and transmission/ retransmission after an Handover	8.4.0	8.5.0
	RP-43	RP-090130	0071	-	Corrections on PDCP services and functions	8.4.0	8.5.0
	RP-43	RP-090130	0077	-	PDCP Control PDU as Data Available for transmission in PDCP	8.4.0	8.5.0
2009-06	RP-44	RP-090515	0078	1	PDCP Status Report	8.5.0	8.6.0
	RP-44	RP-090515	0079	1	Correction to PDCP PDU submission condition in lower layer re-establishment	8.5.0	8.6.0
	RP-44	RP-090515	0080	2	Minor correction and clarification to 36.323	8.5.0	8.6.0
2009-12	RP-46	-	-		Upgrade to the Release 9 - no technical change	8.6.0	9.0.0
2010-12	RP-50	-	-		Upgrade to the Release 10 - no technical change	9.0.0	10.0.0
2011-03	RP-51	RP-110280	0086	-	Clarification on the number of ROHC instances in a PDCP entity	10.0.0	10.1.0
	RP-51	RP-110291	0087	-	Addition of integrity protection of DRBs in PDCP for RNs	10.0.0	10.1.0
2012-03	RP-57	RP-121377	0099	1	Introduction of Carrier aggregation enhancements	10.1.0	11.0.0
2012-12	RP-58	RP-121959	0100	-	CR to 36.323 on introducing ROHC context continue for intra-ENB handover	11.0.0	11.1.0
	RP-58	RP-121959	0104	1	ROHC mode upon handover	11.0.0	11.1.0
	RP-58	RP-121936	0106	-	Prevention of HFN de-synchronization due to PDCP SN over-allocation	11.0.0	11.1.0
2013-03	RP-59	RP-130248	0109	-	ROHC mode upon handover in UM DRB	11.1.0	11.2.0
2014-06	RP-64	RP-140869	0113	-	Clarification of CID reuse	11.2.0	11.3.0
	RP-64	RP-140892	0123	-	ROHC Feedback Handling	11.3.0	12.0.0
2014-09	RP-65	RP-141498	0126	-	Clarification of the decompressor state and mode after PDCP re-establishment	12.0.0	12.1.0
2014-12	RP-66	RP-142135	0128	1	Introduction of dual connectivity in PDCP	12.1.0	12.2.0
2015-03	RP-67	RP-150373	0133	-	Reconfiguration of PDCP reordering timer	12.2.0	12.3.0
	RP-67	RP-150374	0135	-	Introduction of ProSe Direct Communication	12.2.0	12.3.0

2015-06	RP-68	RP-150921	0137	-	COUNT derivation in ProSe	12.3.0	12.4.0
	RP-68	RP-150921	0138	-	Miscellaneous corrections for DC	12.3.0	12.4.0
	RP-68	RP-150921	0139	-	BSR Triggering for Split Bearers	12.3.0	12.4.0
2015-12	RP-70	RP-152053	0145	-	Corrections to Sidelink	12.4.0	12.5.0
	RP-70	RP-152053	0144	1	Update to Services expected from Lower Layers in DC	12.4.0	12.5.0
2015-12	RP-70	RP-152074	0146	-	Introduction of UL split bearer in PDCP	12.5.0	13.0.0
	RP-70	RP-152071	0148	1	Introduction of enhanced CA in PDCP	12.5.0	13.0.0
	RP-70	RP-152072	0149	2	Introducing enhanced ProSe	12.5.0	13.0.0

History

Document history		
V13.0.0	January 2016	Publication