ETSI TS 138 323 V15.5.0 (2019-05)

TECHNICAL SPECIFICATION

5G;
NR;
Packet Data Convergence Protocol (PDCP) specification
(3GPP TS 38.323 version 15.5.0 Release 15)

Reference
RTS/TSGR-0238323vf50

Keywords
5G

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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 38.300: "NG Radio Access Network; Overall description".

[3] 3GPP TS 38.331: "NR Radio Resource Control (RRC); Protocol Specification".

[4] 3GPP TS 38.321: "NR Medium Access Control (MAC) protocol specification".

[5] 3GPP TS 38.322: "NR Radio Link Control (RLC) protocol specification".

[6] 3GPP TS 33.501: "Security Architecture and Procedures for 5G System ".

[7] IETF RFC 5795: "The RObust Header Compression (ROHC) Framework".

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

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

[10] IETF RFC 6846: "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)".

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

[12] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA) Medium Access Control (MAC) protocol specification".

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].

AM DRB: a data radio bearer which utilizes RLC AM.

Non-split bearer: a bearer whose radio protocols are located in either the MgNB or the SgNB to use MgNB or SgNB resource, respectively.

PDCP data volume: the amount of data available for transmission in a PDCP entity.

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

UM DRB: a data radio bearer which utilizes RLC UM.

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
CID	Context Identifier
DRB	Data Radio Bearer carrying user plane data
gNB	NR Node B
HFN	Hyper Frame Number
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Medium Access Control
MAC-I	Message Authentication Code for Integrity
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
RB	Radio Bearer
RFC	Request For Comments
RLC	Radio Link Control
ROHC	RObust Header Compression
RRC	Radio Resource Control
RTP	Real Time Protocol
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.

4.2 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 TS 38.300 [2].

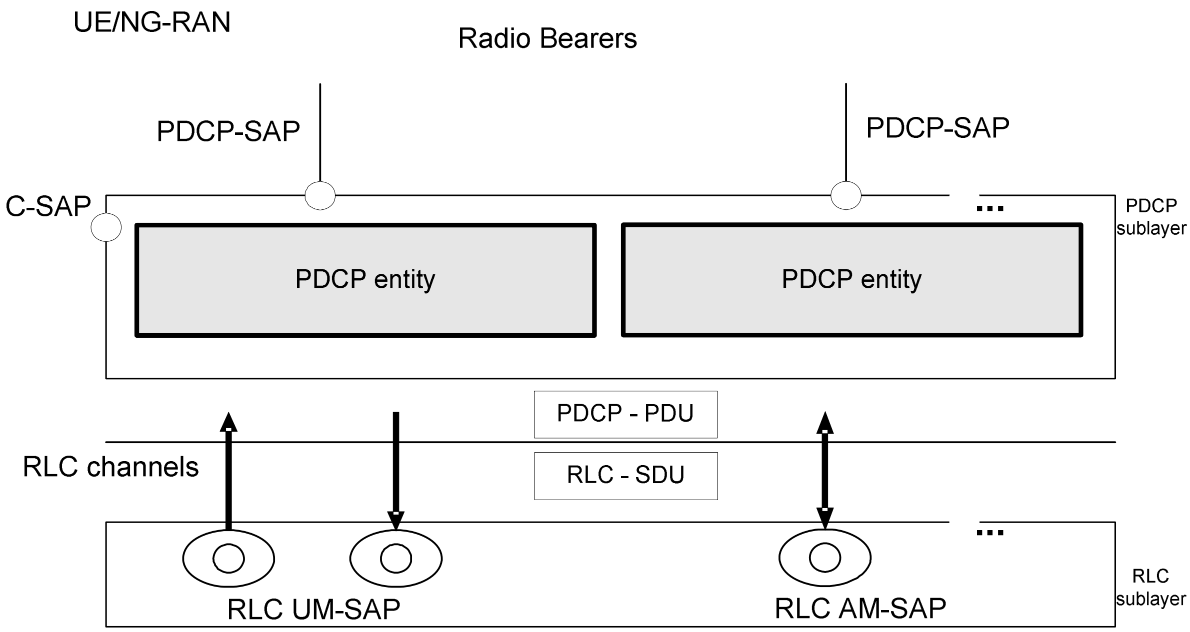

Figure 4.2.1-1: PDCP layer, structure view

The PDCP sublayer is configured by upper layers TS 38.331 [3]. The PDCP sublayer is used for RBs mapped on DCCH and DTCH type of logical channels. The PDCP sublayer is not used for any other type of logical channels.

Each RB (except for SRB0) is associated with one PDCP entity. Each PDCP entity is associated with one, two, or four RLC entities depending on the RB characteristic (e.g uni-directional/bi-directional or split/non-split) or RLC mode. For non-split bearers, each PDCP entity is associated with one UM RLC entity, two UM RLC entities (one for each direction), or one AM RLC entity. For split bearers, each PDCP entity is associated with two UM RLC entities (for same direction), four UM RLC entities (two for each direction), or two AM RLC entities (for same direction).

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.

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 TS 38.300 [2].

For split bearers, routing is performed in the transmitting PDCP entity.

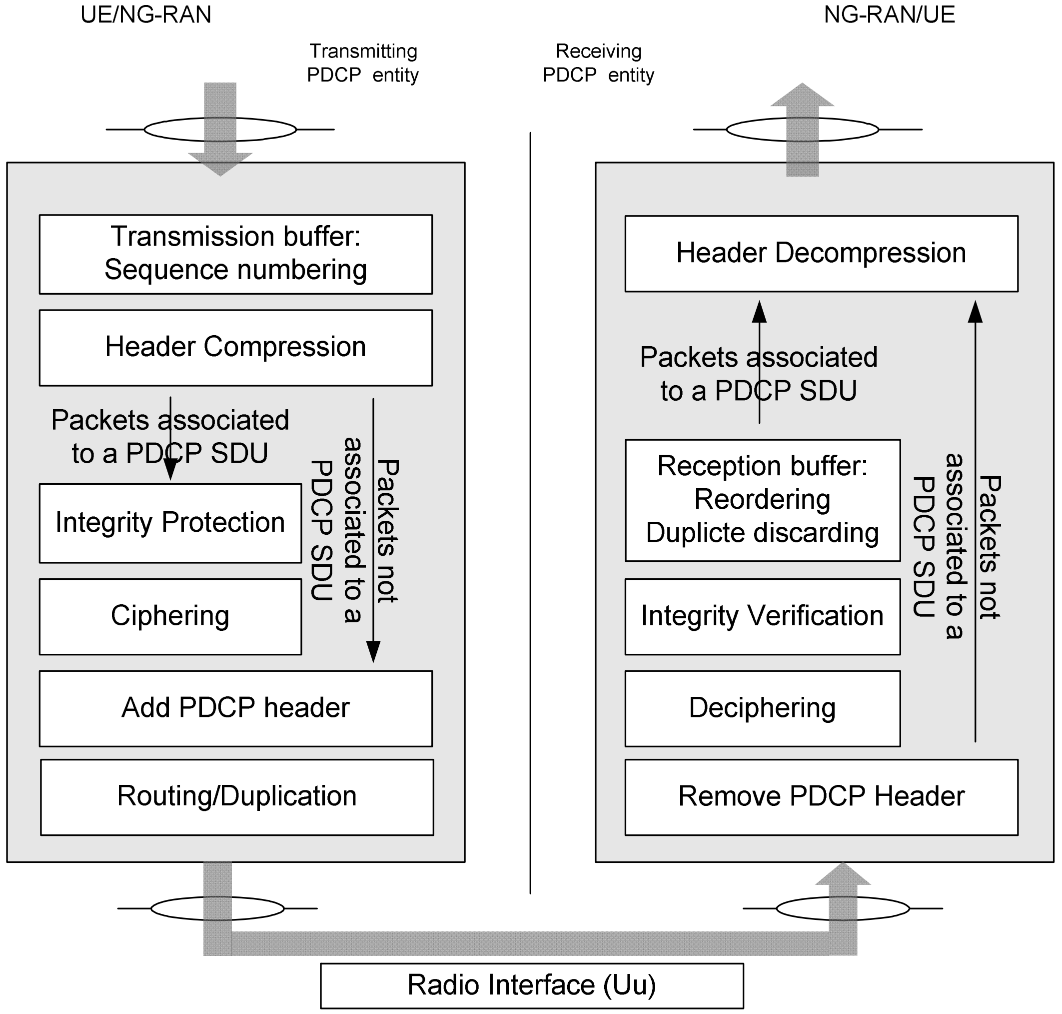

Figure 4.2.2-1: PDCP layer, functional view

4.3 Services

4.3.1 Services provided to upper layers

The PDCP layer provides its services to the RRC or SDAP layers. 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 9000 bytes. The maximum supported size of a PDCP Control PDU is 9000 bytes.

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 TS 38.322 [5]):

- acknowledged data transfer service, including indication of successful delivery of PDCP PDUs;
- unacknowledged data transfer service.

4.4 Functions

The PDCP layer supports the following functions:

- transfer of data (user plane or control plane);
- maintenance of PDCP SNs;
- header compression and decompression using the ROHC protocol;
- ciphering and deciphering;
- integrity protection and integrity verification;
- timer based SDU discard;
- for split bearers, routing;
- duplication;
- reordering and in-order delivery;
- out-of-order delivery;
- duplicate discarding.

5 Procedures

5.1 PDCP entity handling

5.1.1 PDCP entity establishment

When upper layers request a PDCP entity establishment for a radio bearer, the UE shall:

- establish a PDCP entity for the radio bearer;
- set the state variables of the PDCP entity to initial values;
- follow the procedures in subclause 5.2.

5.1.2 PDCP entity re-establishment

When upper layers request a PDCP entity re-establishment, the UE shall additionally perform once the procedures described in this section. After performing the procedures in this section, the UE shall follow the procedures in subclause 5.2.

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

- for UM DRBs and AM DRBs, reset the header compression protocol for uplink and start with an IR state in U-mode (as defined in RFC 3095 [8] and RFC 4815 [9]) if *drb-ContinueROHC* is not configured in TS 38.331 [3];
- for UM DRBs and SRBs, set TX_NEXT to the initial value;
- for SRBs, discard all stored PDCP SDUs and PDCP PDUs;
- apply the ciphering algorithm and key provided by upper layers during the PDCP entity re-establishment procedure;

- apply the integrity protection algorithm and key provided by upper layers during the PDCP entity re-establishment procedure;
- for UM DRBs, for each PDCP SDU already associated with a PDCP SN but for which a corresponding PDU has not previously been submitted to lower layers, and;
- for suspended AM DRBs, from the first PDCP SDU for which the successful delivery of the corresponding PDCP Data PDU has not been confirmed by lower layers, for each PDCP SDU already associated with a PDCP SN:
  - 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 without restarting the *discardTimer*, as specified in subclause 5.2.1;
- for AM DRBs which were not suspended, from the first PDCP SDU for which the successful delivery of the corresponding PDCP Data 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 entity re-establishment as specified below:
  - perform header compression of the PDCP SDU as specified in the subclause 5.7.4;
  - perform integrity protection and ciphering of the PDCP SDU using the COUNT value associated with this PDCP SDU as specified in the subclause 5.9 and 5.8;
  - submit the resulting PDCP Data PDU to lower layer, as specified in subclause 5.2.1.

When upper layers request a PDCP entity re-establishment, the receiving PDCP entity 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 5.2.2.1;
- for SRBs, discard all stored PDCP SDUs and PDCP PDUs;
- for SRBs and UM DRBs, if *t-Reordering* is running:
  - stop and reset *t-Reordering*;
  - for UM DRBs, deliver all stored PDCP SDUs to the upper layers in ascending order of associated COUNT values after performing header decompression;
- for AM DRBs, perform header decompression for all stored PDCP SDUs if *drb-ContinueROHC* is not configured in TS 38.331 [3];
- for UM DRBs and AM DRBs, reset the header compression protocol for downlink and start with NC state in U-mode (as defined in RFC 3095 [8] and RFC 4815 [9]) if *drb-ContinueROHC* is not configured in TS 38.331 [3];
- for UM DRBs and SRBs, set RX_NEXT and RX_DELIV to the initial value;
- apply the ciphering algorithm and key provided by upper layers during the PDCP entity re-establishment procedure;
- apply the integrity protection algorithm and key provided by upper layers during the PDCP entity re-establishment procedure.

5.1.3 PDCP entity release

When upper layers request a PDCP entity release for a radio bearer, the UE shall:

- discard all stored PDCP SDUs and PDCP PDUs in the transmitting PDCP entity;
- for UM DRBs and AM DRBs, deliver the PDCP SDUs stored in the receiving PDCP entity to upper layers in ascending order of associated COUNT values after performing header decompression, if not decompressed before;
- release the PDCP entity for the radio bearer.

5.1.4 PDCP entity suspend

When upper layers request a PDCP entity suspend, the transmitting PDCP entity shall:

- set TX_NEXT to the initial value;
- discard all stored PDCP PDUs;

When upper layers request a PDCP entity suspend, the receiving PDCP entity shall:

- if t-*Reordering* is running:
  - stop and reset *t-Reordering*;
  - deliver all stored PDCP SDUs to the upper layers in ascending order of associated COUNT values after performing header decompression;
- set RX_NEXT and RX_DELIV to the initial value.

5.2 Data transfer

5.2.1 Transmit operation

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

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

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

- associate the COUNT value corresponding to TX_NEXT to this PDCP SDU;

NOTE 1: 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 as specified in the subclause 5.7.4;
- perform integrity protection, and ciphering using the TX_NEXT as specified in the subclause 5.9 and 5.8, respectively;
- set the PDCP SN of the PDCP Data PDU to TX_NEXT modulo $2^{[pdcp\text{-}SN\text{-}SizeUL]}$;
- increment TX_NEXT by one;
- submit the resulting PDCP Data PDU to lower layer as specified below.

When submitting a PDCP PDU to lower layer, the transmitting PDCP entity shall:

- if the transmitting PDCP entity is associated with one RLC entity:
  - submit the PDCP PDU to the associated RLC entity;
- else, if the transmitting PDCP entity is associated with two RLC entities:
  - if the PDCP duplication is activated:
    - if the PDCP PDU is a PDCP Data PDU:
      - duplicate the PDCP Data PDU and submit the PDCP Data PDU to both associated RLC entities;
    - else:
      - submit the PDCP Control PDU to the primary RLC entity;

- else:
  - if the two associated RLC entities belong to the different Cell Groups; and
  - if the total amount of PDCP data volume and RLC data volume pending for initial transmission (as specified in TS 38.322 [5]) in the two associated RLC entities is equal to or larger than *ul-DataSplitThreshold*:
    - submit the PDCP PDU to either the primary RLC entity or the secondary RLC entity;
  - else:
    - submit the PDCP PDU to the primary RLC entity.

NOTE 2: If the transmitting PDCP entity is associated with two RLC entities, the UE should minimize the amount of PDCP PDUs submitted to lower layers before receiving request from lower layers and minimize the PDCP SN gap between PDCP PDUs submitted to two associated RLC entities to minimize PDCP reordering delay in the receiving PDCP entity.

5.2.2 Receive operation

5.2.2.1 Actions when a PDCP Data PDU is received from lower layers

In this section, following definitions are used:

- HFN(State Variable): the HFN part (i.e. the number of most significant bits equal to HFN length) of the State Variable;
- SN(State Variable): the SN part (i.e. the number of least significant bits equal to PDCP SN length) of the State Variable;
- RCVD_SN: the PDCP SN of the received PDCP Data PDU, included in the PDU header;
- RCVD_HFN: the HFN of the received PDCP Data PDU, calculated by the receiving PDCP entity;
- RCVD_COUNT: the COUNT of the received PDCP Data PDU = [RCVD_HFN, RCVD_SN].

At reception of a PDCP Data PDU from lower layers, the receiving PDCP entity shall determine the COUNT value of the received PDCP Data PDU, i.e. RCVD_COUNT, as follows:

- if RCVD_SN < SN(RX_DELIV) – Window_Size:
  - RCVD_HFN = HFN(RX_DELIV) + 1.
- else if RCVD_SN >= SN(RX_DELIV) + Window_Size:
  - RCVD_HFN = HFN(RX_DELIV) – 1.
- else:
  - RCVD_HFN = HFN(RX_DELIV);
- RCVD_COUNT = [RCVD_HFN, RCVD_SN].

After determining the COUNT value of the received PDCP Data PDU = RCVD_COUNT, the receiving PDCP entity shall:

- perform deciphering and integrity verification of the PDCP Data PDU using COUNT = RCVD_COUNT;
  - if integrity verification fails:
    - indicate the integrity verification failure to upper layer;
    - discard the PDCP Data PDU;
- if RCVD_COUNT < RX_DELIV; or

- if the PDCP Data PDU with COUNT = RCVD_COUNT has been received before:
  - discard the PDCP Data PDU;

If the received PDCP Data PDU with COUNT value = RCVD_COUNT is not discarded above, the receiving PDCP entity shall:

- store the resulting PDCP SDU in the reception buffer;
- if RCVD_COUNT >= RX_NEXT:
  - update RX_NEXT to RCVD_COUNT + 1.
- if *outOfOrderDelivery* is configured:
  - deliver the resulting PDCP SDU to upper layers.
- if RCVD_COUNT = RX_DELIV:
  - deliver to upper layers in ascending order of the associated COUNT value after performing header decompression, if not decompressed before;
    - all stored PDCP SDU(s) with consecutively associated COUNT value(s) starting from COUNT = RX_DELIV;
  - update RX_DELIV to the COUNT value of the first PDCP SDU which has not been delivered to upper layers, with COUNT value > RX_DELIV;
- if *t-Reordering* is running, and if RX_DELIV >= RX_REORD:
  - stop and reset *t-Reordering*.
- if *t-Reordering* is not running (includes the case when *t-Reordering* is stopped due to actions above), and RX_DELIV < RX_NEXT:
  - update RX_REORD to RX_NEXT;
  - start *t-Reordering*.

5.2.2.2 Actions when a *t-Reordering* expires

When *t-Reordering* expires, the receiving PDCP entity shall:

- deliver to upper layers in ascending order of the associated COUNT value after performing header decompression, if not decompressed before:
  - all stored PDCP SDU(s) with associated COUNT value(s) < RX_REORD;
  - all stored PDCP SDU(s) with consecutively associated COUNT value(s) starting from RX_REORD;
- update RX_DELIV to the COUNT value of the first PDCP SDU which has not been delivered to upper layers, with COUNT value >= RX_REORD;
- if RX_DELIV < RX_NEXT:
  - update RX_REORD to RX_NEXT;
  - start *t-Reordering*.

5.2.2.3 Actions 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 receiving PDCP entity shall:

- update RX_REORD to RX_NEXT;

- stop and restart *t-Reordering*.

5.3 SDU discard

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

For SRBs, when upper layers request a PDCP SDU discard, the PDCP entity shall discard all stored PDCP SDUs and PDCP PDUs.

NOTE: Discarding a PDCP SDU already associated with a PDCP SN causes a SN gap in the transmitted PDCP Data 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.

5.4 Status reporting

5.4.1 Transmit operation

For AM DRBs configured by upper layers to send a PDCP status report in the uplink (*statusReportRequired* in TS 38.331 [3]), the receiving PDCP entity shall trigger a PDCP status report when:

- upper layer requests a PDCP entity re-establishment;
- upper layer requests a PDCP data recovery.

If a PDCP status report is triggered, the receiving PDCP entity shall:

- compile a PDCP status report as indicated below by:
  - setting the FMC field to RX_DELIV;
  - if RX_DELIV < RX_NEXT:
    - allocating a Bitmap field of length in bits equal to the number of COUNTs 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 9000 bytes, whichever comes first;
    - setting in the bitmap field as '0' for all PDCP SDUs that have not been received, and optionally PDCP SDUs for which decompression have failed;
    - setting in the bitmap field as '1' for all PDCP SDUs that have been received;
- submit the PDCP status report to lower layers as the first PDCP PDU for transmission via the transmitting PDCP entity as specified in subclause 5.2.1.

5.4.2 Receive operation

For AM DRBs, when a PDCP status report is received in the downlink, the transmitting PDCP entity shall:

- consider for each PDCP SDU, if any, with the bit in the bitmap set to '1', or with the associated COUNT value less than the value of FMC field as successfully delivered, and discard the PDCP SDU as specified in the subclause 5.3.

5.5 Data recovery

For AM DRBs, when upper layers request a PDCP data recovery for a radio bearer, the transmitting PDCP entity shall:

- perform retransmission of all the PDCP Data PDUs previously submitted to re-established or released AM RLC entity in ascending order of the associated COUNT values for which the successful delivery has not been confirmed by lower layers, following the data submission procedure in subclause 5.2.1.

After performing the above procedures, the transmitting PDCP entity shall follow the procedures in subclause 5.2.1.

5.6 Data volume calculation

For the purpose of MAC buffer status reporting, the transmitting PDCP entity shall consider the following as PDCP data volume:

- the PDCP SDUs for which no PDCP Data PDUs have been constructed;
- the PDCP Data PDUs that have not been submitted to lower layers;
- the PDCP Control PDUs;
- for AM DRBs, the PDCP SDUs to be retransmitted according to subclause 5.1.2;
- for AM DRBs, the PDCP Data PDUs to be retransmitted according to subclause 5.5.

If the transmitting PDCP entity is associated with two RLC entities, when indicating the PDCP data volume to a MAC entity for BSR triggering and Buffer Size calculation (as specified in TS 38.321 [4] and TS 36.321 [12]), the transmitting PDCP entity shall:

- if the PDCP duplication is activated:
  - indicate the PDCP data volume to the MAC entity associated with the primary RLC entity;
  - indicate the PDCP data volume excluding the PDCP Control PDU to the MAC entity associated with the secondary RLC entity;
- else:
  - if the two associated RLC entities belong to the different Cell Groups; and
  - if the total amount of PDCP data volume and RLC data volume pending for initial transmission (as specified in TS 38.322 [5]) in the two associated RLC entities is equal to or larger than *ul-DataSplitThreshold*:
    - indicate the PDCP data volume to both the MAC entity associated with the primary RLC entity and the MAC entity associated with the secondary RLC entity;
  - else:
    - indicate the PDCP data volume to the MAC entity associated with the primary RLC entity;
    - indicate the PDCP data volume as 0 to the MAC entity associated with the secondary RLC entity.

5.7 Header compression and decompression

5.7.1 Supported header compression protocols and profiles

The header compression protocol is based on the Robust Header Compression (ROHC) framework defined in RFC 5795 [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 defined in RFC 5795 [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 5.7.1-1: Supported header compression protocols and profiles

Profile Identifier	Usage	Reference
0x0000	No compression	RFC 5795
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 6846
0x0101	RTP/UDP/IP	RFC 5225
0x0102	UDP/IP	RFC 5225
0x0103	ESP/IP	RFC 5225
0x0104	IP	RFC 5225

5.7.2 Configuration of header compression

PDCP entities associated with DRBs can be configured by upper layers TS 38.331 [3] to use header compression. Each PDCP entity carrying user plane data may be configured to use header compression. 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.

5.7.3 Protocol parameters

RFC 5795 [7] has configuration parameters that are mandatory and that must be configured by upper layers between compressor and decompressor peers ; these parameters define the ROHC channel. The ROHC channel is a unidirectional channel, i.e. if *rohc* is configured there is one channel for the downlink and one for the uplink, and if *uplinkOnlyROHC* is configured there is only one channel for the uplink. There is thus one set of parameters for each channel, and if *rohc* is configured 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* in TS 38.331 [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 clause 5.7.1. The parameter PROFILES is configured by upper layers (*profiles* for uplink and downlink in TS 38.331 [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.

5.7.4 Header compression

If header compression is configured, 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.

A compressed packet is associated with the same PDCP SN and COUNT value as the related PDCP SDU. The header compression is not applicable to the SDAP header and the SDAP Control PDU if included in the PDCP SDU.

Interspersed ROHC feedback 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.

5.7.5 Header decompression

If header compression is configured by upper layers for PDCP entities associated with user plane data, the PDCP Data PDUs are decompressed by the header compression protocol after performing deciphering as explained in the subclause 5.8. The header decompression is not applicable to the SDAP header and the SDAP Control PDU if included in the PDCP Data PDU.

5.7.6 PDCP Control PDU for interspersed ROHC feedback

5.7.6.1 Transmit Operation

When an interspersed ROHC feedback is generated by the header compression protocol, the transmitting PDCP entity shall:

- submit to lower layers the corresponding PDCP Control PDU as specified in subclause 6.2.3.2 i.e. without associating a PDCP SN, nor performing ciphering.

5.7.6.2 Receive Operation

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

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

5.8 Ciphering and deciphering

The ciphering function includes both ciphering and deciphering and is performed in PDCP, if configured. The data unit that is ciphered is the MAC-I (see subclause 6.3.4) and the data part of the PDCP Data PDU (see subclause 6.3.3) except the SDAP header and the SDAP Control PDU if included in the PDCP SDU. The 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 TS 38.331 [3] and the ciphering method shall be applied as specified in TS 33.501 [6].

The ciphering function is activated/suspended/resumed by upper layers TS 38.331 [3]. When security is activated and not suspended, the ciphering function shall be applied to all PDCP Data PDUs indicated by upper layers TS 38.331 [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 TS 33.501 [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 TS 33.501 [6]).The parameters required by PDCP which are provided by upper layers TS 38.331 [3] are listed below:

- BEARER (defined as the radio bearer identifier in TS 33.501 [6]. It will use the value RB identity –1 as in TS 38.331 [3]);

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

5.9 Integrity protection and verification

The integrity protection function includes both integrity protection and integrity verification and is performed in PDCP, if configured. The data unit that is integrity protected is the PDU header and the data part of the PDU before ciphering. The integrity protection is always applied to PDCP Data PDUs of SRBs. The integrity protection is applied to PDCP Data PDUs of DRBs for which integrity protection is configured. The integrity protection is not applicable to PDCP Control PDUs.

The integrity protection algorithm and key to be used by the PDCP entity are configured by upper layers TS 38.331 [3] and the integrity protection method shall be applied as specified in TS 33.501 [6].

The integrity protection function is activated/suspended/resumed by upper layers TS 38.331 [3]. When security is activated and not suspended, the integrity protection function shall be applied to all PDUs including and subsequent to the PDU indicated by upper layers TS 38.331 [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 TS 33.501 [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 TS 33.501 [6]). The parameters required by PDCP which are provided by upper layers TS 38.331 [3] are listed below:

- BEARER (defined as the radio bearer identifier in TS 33.501 [6]. It will use the value RB identity –1 as in TS 38.331 [3]);
- KEY (the integrity protection keys for the control plane and for the user plane are K_{RRCint} and K_{UPint}, respectively).

At transmission, the UE computes the value of the MAC-I field and at reception it verifies the integrity of the PDCP Data 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.

5.10 Handling of unknown, unforeseen, and erroneous protocol data

When a PDCP PDU that contains reserved or invalid values is received, the receiving PDCP entity shall:

- discard the received PDU.

5.11 PDCP duplication

5.11.1 Activation/Deactivation of PDCP duplication

For the PDCP entity configured with *pdcp-Duplication*, the transmitting PDCP entity shall:

- for SRBs:
  - activate the PDCP duplication;
- for DRBs:
  - if the activation of PDCP duplication is indicated:
    - activate the PDCP duplication;
  - if the deactivation of PDCP duplication is indicated:
    - deactivate the PDCP duplication.

5.11.2 Duplicate PDU discard

For the PDCP entity configured with *pdcp-Duplication*, the transmitting PDCP entity shall:

- if the successful delivery of a PDCP Data PDU is confirmed by one of the two associated AM RLC entities:
  - indicate to the other AM RLC entity to discard the duplicated PDCP Data PDU;
- if the deactivation of PDCP duplication is indicated:
  - indicate to the secondary RLC entity to discard all duplicated PDCP Data PDUs.

6 Protocol data units, formats, and parameters

6.1 Protocol data units

6.1.1 Data PDU

The PDCP Data PDU is used to convey one or more of followings in addition to the PDU header:

- user plane data;
- control plane data;
- a MAC-I.

6.1.2 Control PDU

The PDCP Control PDU is used to convey one of followings in addition to the PDU header:

- a PDCP status report;
- an 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 subclause 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 Data PDU from the first bit onward.

6.2.2 Data PDU

6.2.2.1 Data PDU for SRBs

Figure 6.2.2.1-1 shows the format of the PDCP Data PDU with 12 bits PDCP SN. This format is applicable for SRBs.

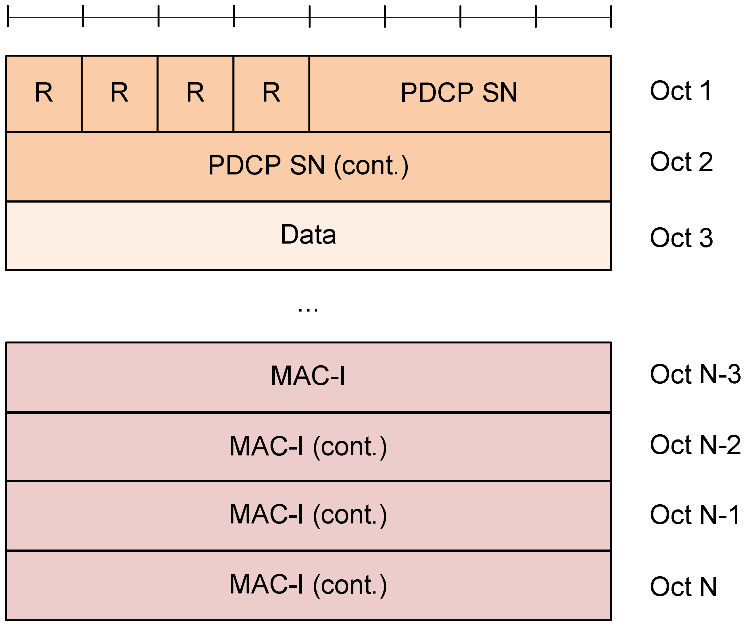

Figure 6.2.2.1-1: PDCP Data PDU format for SRBs

6.2.2.2 Data PDU for DRBs with 12 bits PDCP SN

Figure 6.2.2.2-1 shows the format of the PDCP Data PDU with 12 bits PDCP SN. This format is applicable for UM DRBs and AM DRBs.

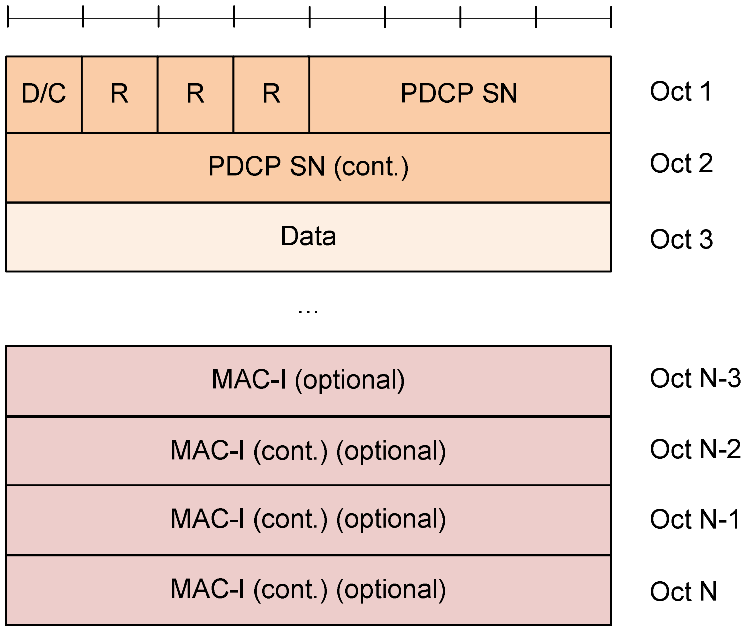

Figure 6.2.2.2-1: PDCP Data PDU format with 12 bits PDCP SN

6.2.2.3 Data PDU for DRBs with 18 bits PDCP SN

Figure 6.2.2.3-1 shows the format of the PDCP Data PDU with 18 bits PDCP SN. This format is applicable for UM DRBs and AM DRBs.

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

Figure 6.2.2.3-1: PDCP Data PDU format for DRBs with 18 bits PDCP SN

6.2.3 Control PDU

6.2.3.1 Control PDU for PDCP status report

Figure 6.2.3.1-1 shows the format of the PDCP Control PDU carrying one PDCP status report. This format is applicable for AM DRBs.

D/C	PDU Type	R	R	R	R	Oct 1
FMC						Oct 2
FMC (cont.)						Oct 3
FMC (cont.)						Oct 4
FMC (cont.)						Oct 5
$Bitmap_1$ (optional)						Oct 6
...						
$Bitmap_N$ (optional)						Oct 5+N

Figure 6.2.3.1-1: PDCP Control PDU format for PDCP status report

6.2.3.2 Control PDU for interspersed ROHC feedback

Figure 6.2.3.2-1 shows the format of the PDCP Control PDU carrying one interspersed ROHC feedback. This format is applicable for UM DRBs and AM DRBs.

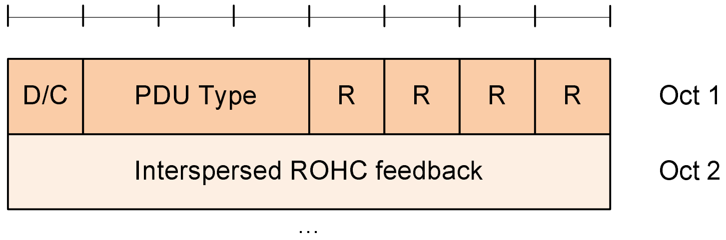

Figure 6.2.3.2-1: PDCP Control PDU format for interspersed ROHC feedback

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: 12, or 18 bits as indicated in table 6.3.2.1. The length of the PDCP SN is configured by upper layers (*pdcp-SN-SizeUL* or *pdcp-SN-SizeDL* in TS 38.331 [3]).

Table 6.3.2-1: PDCP SN length

Length	Description
12	UM DRBs, AM DRBs, and SRBs
18	UM DRBs, and AM DRBs

6.3.3 Data

Length: Variable

This field includes one of the followings:

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

6.3.4 MAC-I

Length: 32 bits

This field carries a message authentication code calculated as specified in subclause 5.9.

For SRBs, the MAC-I field is always present. If integrity protection is not configured, the MAC-I field is still present but should be padded with padding bits set to 0.

For DRBs, the MAC-I field is present only when the DRB is configured with integrity protection.

6.3.5 COUNT

Length: 32 bits

The COUNT value is composed of a HFN and the PDCP SN. The size of the HFN part in bits is equal to 32 minus the length of the PDCP SN.

HFN	PDCP SN

Figure 6.3.5-1: Format of COUNT

NOTE: COUNT does not wrap around.

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

This field indicates whether the corresponding PDCP PDU is a PDCP Data PDU or a PDCP Control PDU.

Table 6.3.7-1: D/C field

Bit	Description
0	Control PDU
1	Data PDU

6.3.8 PDU type

Length: 3 bits

This field indicates the type of control information included in the corresponding PDCP Control PDU.

Table 6.3.8-1: PDU type

Bit	Description
000	PDCP status report
001	Interspersed ROHC feedback
010-111	Reserved

6.3.9 FMC

Length: 32 bits

First Missing COUNT. This field indicates the COUNT value of the first missing PDCP SDU within the reordering window, i.e. RX_DELIV.

6.3.10 Bitmap

Length: Variable. The length of the bitmap field can be 0.

This field indicates which SDUs are missing and which SDUs are correctly received in the receiving PDCP entity. 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.

Table 6.3.10-1 Bitmap

Bit	Description
0	PDCP SDU with COUNT = (FMC + bit position) modulo 2^{32} is missing.
1	PDCP SDU with COUNT = (FMC + bit position) modulo 2^{32} is correctly received.

6.3.11 Interspersed ROHC feedback

Length: Variable

This field contains one ROHC packet with only feedback, i.e. a ROHC packet that is not associated with a PDCP SDU as defined in subclause 5.7.4.

7 State 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. The state variables defined in this subclause are normative.

All state variables are non-negative integers, and take values from 0 to $[2^{32} – 1]$.

PDCP Data PDUs are numbered integer sequence numbers (SN) cycling through the field: 0 to $[2^{[pdcp\text{-}SN\text{-}SizeUL]} – 1]$ or 0 to $[2^{[pdcp\text{-}SN\text{-}SizeDL]} – 1]$.

The transmitting PDCP entity shall maintain the following state variables:

a) TX_NEXT

This state variable indicates the COUNT value of the next PDCP SDU to be transmitted. The initial value is 0.

The receiving PDCP entity shall maintain the following state variables:

a) RX_NEXT

This state variable indicates the COUNT value of the next PDCP SDU expected to be received. The initial value is 0.

b) RX_DELIV

This state variable indicates the COUNT value of the first PDCP SDU not delivered to the upper layers, but still waited for. The initial value is 0.

c) RX_REORD

This state variable indicates the COUNT value following the COUNT value associated with the PDCP Data PDU which triggered *t-Reordering*.

7.2 Constants

a) Window_Size

This constant indicates the size of the reordering window. The value equals to $2^{[pdcp\text{-}SN\text{-}SizeDL] – 1}$.

7.3 Timers

The transmitting PDCP entity shall maintain the following timers:

a) *discardTimer*

This timer is configured only for DRBs. The duration of the timer is configured by upper layers TS 38.331 [3]. In the transmitter, a new timer is started upon reception of an SDU from upper layer.

The receiving PDCP entity shall maintain the following timers:

b) *t-Reordering*

The duration of the timer is configured by upper layers TS 38.331 [3]. This timer is used to detect loss of PDCP Data PDUs as specified in the subclause 5.2.2. If *t-Reordering* is running, *t-Reordering* shall not be started additionally, i.e. only one *t-Reordering* per receiving PDCP entity is running at a given time.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New Version**
2017.03	RAN2#97bis	R2-1703512	-	-	-	First version.	x.y.z
2017.04	RAN2#97bis	R2-1703916	-	-	-	Change section name "Retransmission" to "Data recovery"	0.0.1
2017.05	RAN2#98	R2-1704076	-	-	-	Initial draft TS capturing outcome of e-mail discussion [97bis#24]	0.0.5
2017.06	RAN2 NR AH	R2-1706868	-	-	-	Capture agreements made in RAN2#98	0.1.0
2017.08	RAN2 NR AH	R2-1707507	-	-	-	Capture agreements made in RAN2 NR AH#2	0.2.0
2017.08	RAN2#99	R2-1709097	-	-	-	Adding integrity protection in section 5.1.2	0.2.1
2017.08	RAN2#99	R2-1709753	-	-	-	Capture agreements made in RAN2#99	0.3.0
2017.09	RANP#77	RP-171993	-	-	-	Provided for information to RAN	1.0.0
2017.10	RAN2#99bis	R2-1713660	-	-	-	Capture agreements made in RAN2#99bis	1.0.1
2017.11	RAN2#100	R2-1714273	-	-	-	Capture agreements made in RAN2#100	1.1.0
2017.12	RP-78	RP-172335	-	-	-	Provided for approval to RAN	2.0.0
2017/12	RP-78					Upgraded to Rel-15 (MCC)	15.0.0
2018/03	RP-79	RP-180440	0002	1	F	Corrections to PDCP specification	15.1.0
2018/06	RP-80	RP-181215	0006	3	F	Corrections to PDCP specification	15.2.0
	RP-80	RP-181215	0009	1	B	Introduction of PDCP duplication	15.2.0
2018/09	RP-81	RP-181942	0011	4	F	Clarification on PDCP transmission	15.3.0
2018/12	RP-82	RP-182650	0022	1	F	Suspend and resume of security	15.4.0
	RP-82	RP-182655	0023	-	F	Introducing PDCP suspend procedure	15.4.0
	RP-82	RP-182656	0024	-	F	Clarification on ciphering MAC-I	15.4.0
2019/03	RP-83	RP-190544	0025	2	F	Correction on the PDCP re-establishment for AM DRB	15.5.0
	RP-83	RP-190540	0027	1	F	Correction on PDCP SN length	15.5.0

History

Document history		
V15.2.0	September 2018	Publication
V15.3.0	October 2018	Publication
V15.4.0	April 2019	Publication
V15.5.0	May 2019	Publication