Authors: E. Ramos    A. Minaburo
          Ericsson    Acklio

**SCHC over NBIoT**

**Abstract**

   The Static Context Header Compression and Fragmentation (SCHC)
   specification describes header compression and fragmentation
   functionalities for LPWAN (Low Power Wide Area Networks)
   technologies. The Narrowband Internet of Things (NB-IoT)
   architecture may adapt SCHC to improve its capacities.

   This document describes the use of SCHC over the NB-IoT wireless
   access and provides recommendations for the use cases and efficient
   parameterization.

**Status of This Memo**

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at https://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six
   months and may be updated, replaced, or obsoleted by other documents
   at any time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on 30 December 2022.

**Copyright Notice**

**Table of Contents**

## 1. Introduction

The Static Context Header Compression (SCHC) [RFC8724] defines a
header compression scheme and fragmentation functionality suitable
for the Low Power Wide Area Networks (LPWAN) networks described in
[RFC8376]. In a Narrowband Internet of Things (NB-IoT) network,
header compression efficiently brings Internet connectivity to the
Device-User Equipment (Dev-UE). This document describes the SCHC
parameters that support the static context header compression and
fragmentation over the NB-IoT wireless access. This document assumes
functionality for NB-IoT of 3GPP release 15 [_3GPPR15]. Otherwise,
the text explicitly mentions other versions' functionality.

## 2. Terminology

This document will follow the terms defined in [RFC8724], in [RFC8376], and the [TR23720].

   *CIoT. Cellular IoT.

   *NGW-C-SGN. Network Gateway - CIoT Serving Gateway Node.

   *Dev-UE. Device - User Equipment.

   *RGW-eNB. Radio Gateway - Node B. Base Station that controls the UE.

   *EPC. Evolved Packet Connectivity. Core network of 3GPP LTE systems.

   *EUTRAN. Evolved Universal Terrestrial Radio Access Network. Radio access network of LTE-based systems.

   *NGW-MME. Network Gateway - Mobility Management Entity. An entity in charge of handling mobility of the Dev-UE.

   *NB-IoT. Narrowband IoT. A 3GPP LPWAN technology based on the LTE architecture but with additional optimization for IoT and using a Narrowband spectrum frequency.

   *NGW-SGW. Network Gateway - Serving Gateway. It routes and forwards the user data packets through the access network.

   *HSS. Home Subscriber Server. It is a database that performs mobility management.

   *NGW-PGW. Network Gateway - Packet Data Node Gateway. An interface between the internal with the external network.

   *PDU. Protocol Data Unit. A data packet including headers that are transmitted between entities through a protocol.

   *SDU. Service Data Unit. A data packet (PDU) from higher layer protocols used by lower layer protocols as a payload of their own PDUs.

   *IWK-SCEF. InterWorking Service Capabilities Exposure Function. It is used in roaming scenarios, it is located in the Visited PLMN and serves for interconnection with the SCEF of the Home PLMN.

   *NGW-SCEF. Network Gateway - Service Capability Exposure Function. EPC node for exposure of 3GPP network service capabilities to 3rd party applications.

## 3.  Architecture

The Narrowband Internet of Things (NB-IoT) architecture has a
complex structure. It relies on different NGWs from different
providers. It can send data via different paths, each with different
characteristics in terms of bandwidths, acknowledgments, and layer
two reliability and segmentation.

Figure 1 shows this architecture, where the Network Gateway Cellular
Internet of Things Serving Gateway Node (NGW-CSGN) optimizes co-
locating entities in different paths. For example, a Dev-UE using
the path formed by the Network Gateway Mobility Management Entity
(NGW-MME), the NGW-CSGW, and Network Gateway Packet Data Node
Gateway (NGW-PGW) may get a limited bandwidth transmission from a
few bytes/s to one thousand bytes/s only.

Another node introduced in the NB-IoT architecture is the Network
Gateway Service Capability Exposure Function (NGW-SCEF), which
securely exposes service and network capabilities to entities
external to the network operator. OMA and OneM2M define the
northbound APIS [TR33203]. In this case, the path is small for data
transmission. The main functions of the NGW-SCEF are Connectivity
path and Device Monitoring.

```
+---+                              +------+
|Dev| \                 +-----+ ----| HSS  |
|-UE|  \                | NGW |      +------+
+---+   |               |-MME |\__
         \            / +-----+   \
+---+    \+-----+ /     |        +------+
|Dev| ----| RGW |-      |        | NGW- |
|-UE|     |-eNB |       |        | SCEF |---------+
+---+    /+-----+ \     |        +------+         |
      /           \ +------+                      |
     /             \| NGW- |   +-----+   +-----------+
+---+ /             | CSGW |--| NGW-|---|Application|
|Dev|               |      |  | PGW |   |  Server   |
|-UE|               +------+  +-----+   +-----------+
+---+
```
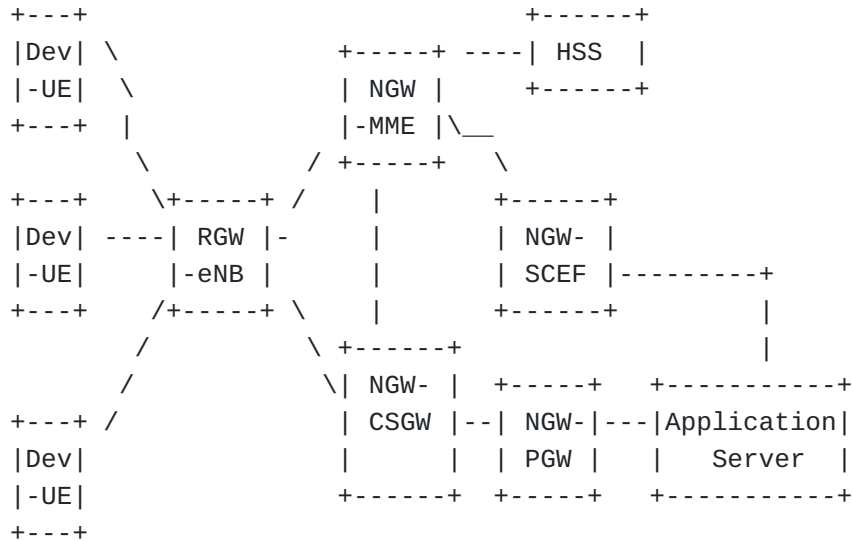
Figure 1: 3GPP network architecture

## 4.  Data Transmission in the 3GPP Architecture

NB-IoT networks deal with end-to-end user data and in-band signaling
between the nodes and functions to configure, control, and monitor
the system functions and behaviors. The signaling data uses a

different path with specific protocols, handling processes, and
entities but can transport end-to-end user data for IoT services. In
contrast, the end-to-end application only transports end-to-end
data.

The maximum recommended 3GPP MTU size is 1358 Bytes. The radio
network protocols limit the packet sizes over the air, including
radio protocol overhead, to 1600 Bytes. However, the recommended MTU
is smaller to avoid fragmentation in the network backbone due to the
payload encryption size (multiple of 16) and the additional core
transport overhead handling.

3GPP standardizes NB-IoT and, in general, the cellular technologies
interfaces and functions. Therefore the introduction of SCHC
entities to Dev-UE, RGW-eNB, and NGW-CSGN needs to be specified in
the NB-IoT standard, which implies that the standard specifying SCHC
support would not be backward compatible. A terminal or a network
supporting a version of the standard without SCHC or implementation
capability (in case of not being standardized as mandatory
capability) cannot utilize SCHC with this approach.

SCHC could be deployed differently depending on where the header
compression and the fragmentation are applied. The SCHC
functionalities can only be used over the radio transmission between
the Dev-UE and the RGW-eNB. Alternatively, the packets transmitted
over the path can use SCHC. When the transmissions go over the NGW-
MME or NGW-SCEF, the NGW-CSGN uses the SCHC entity. For these two
cases, the functions need to be standardized by 3GPP.

Another possibility is to apply SCHC functionalities to the end-to-
end connection or at least up to the operator network edge. SCHC
functionalities are available in the application layer of the Dev-UE
and the Application Servers or a broker function at the edge of the
operator network. The radio network transmits the packets as non-IP
traffic using IP tunneling or SCEF services. Since this option does
not necessarily require 3GPP standardization, it is possible to also
benefit legacy devices with SCHC by using the non-IP transmission
features of the operator network.

## 4.1.  Use of SCHC over the Radio link

Deploying SCHC over the radio link only would require placing it as
part of the protocol stack for data transfer between the Dev-UE and
the RGW-eNB. This stack is the functional layer responsible for
transporting data over the wireless connection and managing radio
resources. There is support for features such as reliability,
segmentation, and concatenation. The transmissions use link
adaptation, meaning that the system will optimize the transport
format used according to the radio conditions, the number of bits to

transmit, and the power and interference constraints. That means
that the number of bits transmitted over the air depends on the
selected Modulation and Coding Schemes (MCS). Transport Block (TB)
transmissions happen in the physical layer at network synchronized
intervals called Transmission Time Interval (TTI). Each Transport
Block has a different MCS and number of bits available to transmit.
The MAC layer [TR36321] defines the Transport Blocks'
characteristics. The Radio link stack shown in Figure 2 comprises
the Packet Data Convergence Protocol (PDCP) [TS36323], Radio Link
Protocol (RLC) [TS36322], Medium Access Control protocol (MAC)
[TR36321], and the Physical Layer [TS36201]. The Appendix gives more
details about these protocols.

### 4.1.1.  SCHC Entities Placing

The current architecture supports header compression in the PDCP
layer using RoHC [RFC5795]. Therefore the architecture can deploy
SCHC header compression entities similarly without the need for
significant changes in the 3GPP specifications.

In this scenario, the RLC layer takes care of fragmentation unless
for the Transparent Mode. When packets exceed the Transport Block
size at transmission, SCHC fragmentation is unnecessary and should
not be used to avoid the additional protocol overhead. The RLC
Transparent Mode is not commonly used while sending IP packets in
the Radio link. However, given the case in the future, SCHC
fragmentation may be used. In that case, a SCHC tile would match the
minimum transport block size minus the PDCP and MAC headers.

```
+---------+                                  +---------+  |
|IP/non-IP+----------------------------------+IP/non-IP+->+
+---------+   |   +--------------+   |   +---------+  |
| PDCP    +-------+ PDCP  | GTP|U +------+ GTP-U    |->+
| (SCHC)  +       + (SCHC)|       +      +          |  |
+---------+   |   +--------------+   |   +---------+  |
| RLC     +-------+ RLC   |UDP/IP +------+ UDP/IP   +->+
+---------+   |   +--------------+   |   +---------+  |
| MAC     +-------+ MAC   | L2    +------+ L2       +->+
+---------+   |   +--------------+   |   +---------+  |
| PHY     +-------+ PHY   | PHY   +------+ PHY      +->+
+---------+       +--------------+      +---------+  |
         C-Uu/                  S1-U              SGi
  Dev-UE             RGW-eNB          NGW-CSGN
         Radio Link
```
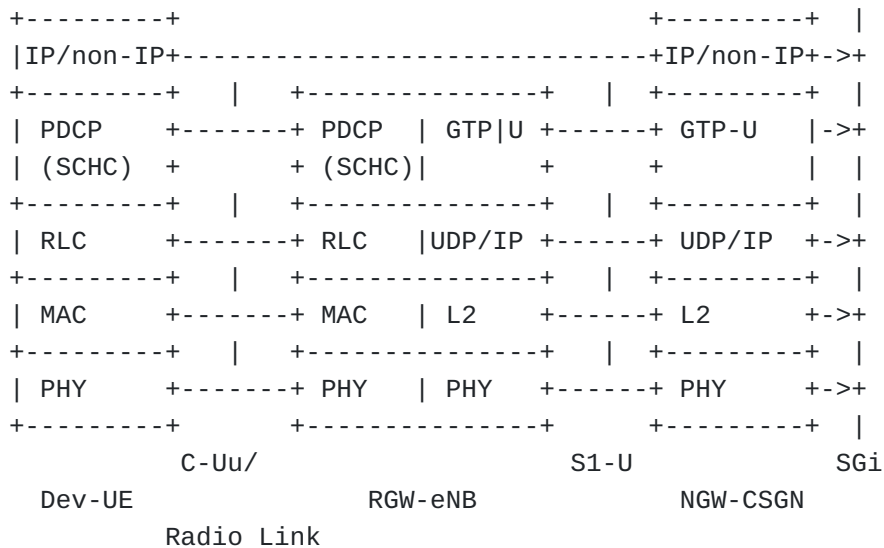
                    Figure 2: SCHC over the Radio link

## 4.2.  Use of SCHC over the No-Access Stratum (NAS)

The NGW-MME conveys mainly control signaling between the Dev-UE and the cellular network [TR24301]. The network transports this traffic on top of the radio link.

This kind of flow supports data transmissions to reduce the overhead when transmitting infrequent small quantities of data. This transmission is known as Data over No-Access Stratum (DoNAS) or Control Plane CIoT EPS optimization. In DoNAS, the Dev-UE uses the pre-established security and can piggyback small uplink data into the initial uplink message and uses an additional message to receive a downlink small data response.

The NGW-MME performs the data encryption from the network side in a DoNAS PDU. Depending on the data type signaled indication (IP or non-IP data), the network allocates an IP address or establishes a direct forwarding path. DoNAS is regulated under rate control upon previous agreement, meaning that a maximum number of bits per unit of time is agreed upon per device subscription beforehand and configured in the device.

The system will use DoNAS when a terminal in a power-saving state requires a short transmission and receives an acknowledgment or short feedback from the network. Depending on the size of buffered data to transmit, the Dev-UE might deploy the connected mode transmissions instead, limiting and controlling the DoNAS transmissions to predefined thresholds and a good resource optimization balance for the terminal and the network. The support for mobility of DoNAS is present but produces additional overhead. The Appendix gives additional details of DoNAS.

### 4.2.1.  SCHC Entities Placing

In this scenario, SCHC may reside in the Non-Access Stratum (NAS) protocol layer. The same principles as for Radio link transmissions apply here as well. Because the NAS protocol already uses RoHC it can adapt SCHC for header compression too. The main difference compared to the radio link is the physical placing of the SCHC entities. On the network side, the NGW-MME resides in the core network and is the terminating node for NAS instead of the RGW-eNB.

```
+--------+                       +--------+--------+  +  +--------+
| IP/    +--+-----------------+--+  IP/   |  IP/   +-----+   IP/  |
| Non-IP |  |                    |  | Non-IP | Non-IP |  |  | Non-IP |
+--------+  |                    |  +----------------+  |  +--------+
| NAS    +----------------------+    NAS  |GTP-C/U +-----+GTP-C/U |
|(SCHC)  |  |                    |  | (SCHC) |        |  |  |        |
+--------+  |  +-----------+    |  +----------------+  |  +--------+
| RRC    +-----+RRC  |S1|AP+-----+ S1|AP  |        |  |  |        |
+--------+  |  +-----------+    |  +--------+  UDP  +-----+  UDP   |
| PDCP*  +-----+PDCP*|SCTP +-----+ SCTP   |        |  |  |        |
+--------+  |  +-----------+    |  +----------------+  |  +--------+
| RLC    +-----+ RLC | IP  +-----+ IP     | IP     +-----+ IP     |
+--------+  |  +-----------+    |  +----------------+  |  +--------+
| MAC    +-----+ MAC | L2  +-----+ L2     | L2     +-----+ L2     |
+--------+  |  +-----------+    |  +----------------+  |  +--------+
| PHY    +--+--+ PHY | PHY +--+--+ PHY    | PHY    +-----+ PHY    |
+--------+     +-----+-----+    +--------+--------+  |  +--------+
         C-Uu/           S1-lite                  SGi
 Dev-UE          RGW-eNB            NGW-MME              NGW-PGW
```
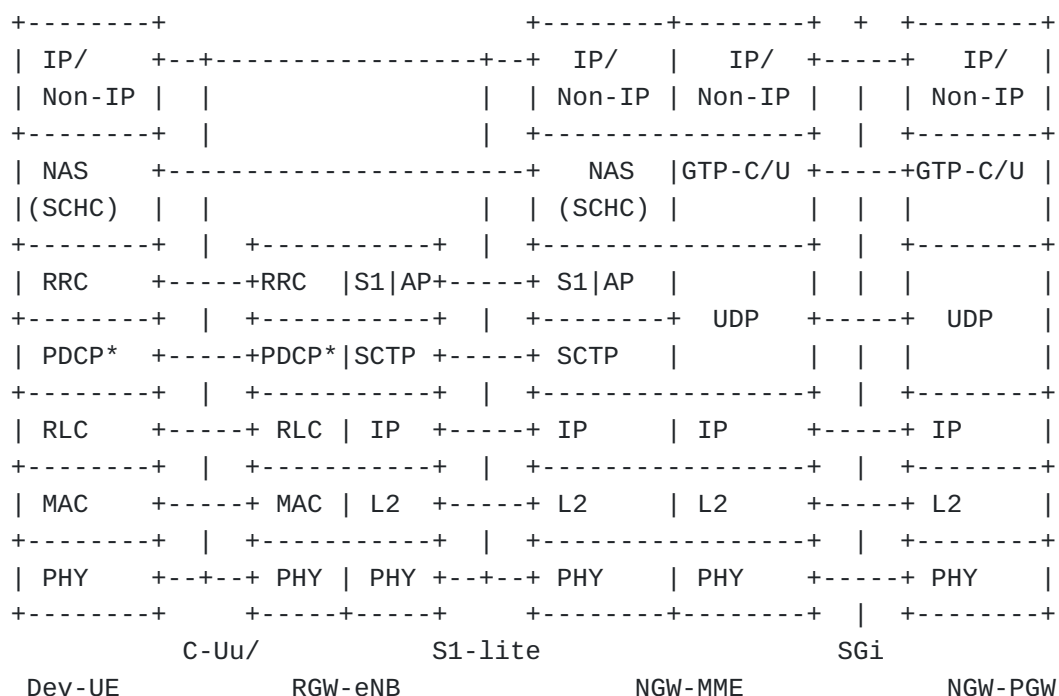
*PDCP is bypassed until AS security is activated TGPP36300.

Figure 3: SCHC entities placement in the 3GPP CIOT radio protocol
                architecture for DoNAS transmissions

**4.2.2.  Parameters for Static Context Header Compression and Fragmentation (SCHC) for the Radio and DONAS.**

These scenarios MUST use SCHC header compression capability to improve the transmission of IPv6 packets. The 3GPP Architecture currently provides Header Compression using the [RFC5795], but using SCHC for IoT applications MUST be considered to improve the device's connectivity.

*SCHC Context initialization RRC (Radio Resource Control) protocol is the main tool used to configure the parameters of the Radio link. It will configure SCHC and the static context distribution as it has made for RoHC operation [TS36323].

*SCHC Rules The network operator in these scenarios defines the number of rules in a context. The operator must be aware of the type of IP traffic that the device will carry out. Implying that the operator might use provision sets of rules compatible with the use case of the device. For devices acting as gateways to other devices, several rules may match the diversity of devices and protocols used by the devices associated with the gateway.

Meanwhile, simpler devices (for example, an electricity meter) may have a predetermined set of fixed protocols and parameters. Additionally, the deployment of IPv6 addresses may force different rules to deal with each case.

*RuleID There is a reasonable assumption of 9 bytes of radio protocol overhead for these transmission scenarios in NB-IoT, where PDCP uses 5 bytes due to header and integrity protection, and RLC and MAC use 4 bytes. The minimum physical Transport Blocks (TB) that can withhold this overhead value according to 3GPP Release 15 specifications are 88, 104, 120, and 144 bits. A transmission optimization may require only one physical layer transmission. SCHC overhead should not exceed the available number of effective bits of the smallest physical TB available. The packets handled by 3GPP networks are byte-aligned, and therefore the minimum payload possible (including padding) is 8 bits. Thus to use the smallest TB, the maximum SCHC header size is 12 bits. These 12 bits must include the Compression Residue in addition to the RuleID. On the other hand, more complex NB-IoT devices (such as a capillarity gateway) might require additional bits to handle the variety and multiple parameters of higher-layer protocols deployed. In that sense, the operator may want to have flexibility on the number and type of rules supported by each device independently, and consequently, these scenarios require a configurable value. The configuration may be part of the operation profile agreed together with the content distribution. The RuleID field size may range from 2 bits, resulting in 4 rules to an 8-bit value that would yield up to 256 rules that can be used together with the operators and seems quite a reasonable maximum limit even for a device acting as a NAT. An application may use a larger RuleID, but it should consider the byte-alignment of the expected Compression Residue. In the minimum TB size case, 2 bits of RuleID leave only 6 bits available for Compression Residue.

*SCHC MAX_PACKET_SIZE The Radio Link can handle the fragmentation of SCHC packets if needed, including reliability. Hence the packet size is limited by the MTU handled by the radio protocols, which corresponds to 1600 bytes for 3GPP Release 15.

*Fragmentation For the Section 4.1 and Section 4.2 scenarios, the SCHC fragmentation functions are disabled. The RLC layer of NB-IoT can segment packets in suitable units that fit the selected transport blocks for transmissions of the physical layer. The block selection is made according to the link adaptation input function in the MAC layer and the quantity of data in the buffer. The link adaptation layer may produce different results at each Time Transmission Interval (TTI), resulting in varying physical transport blocks that depend on the network load, interference,

number of bits transmitted, and QoS. Even if setting a value that
allows the construction of data units following the SCHC tiles
principle, the protocol overhead may be greater or equal to
allowing the Radio link protocols to take care of the
fragmentation natively.

*Fragmentation in RLC Transparent Mode If RLC operates in
Transparent Mode, there could be a case to activate a
fragmentation function together with a light reliability function
such as the ACK-Always mode. In practice, it is uncommon to
transmit radio link data using this configuration. It mainly
targets signaling transmissions. In those cases, the MAC layer
mechanisms ensure reliability, such as repetitions or automatic
retransmissions, and additional reliability might only generate
protocol overhead.

SCHC may reduce radio network protocol overhead in future
operations, support reliable transmissions, and transmit compressed
data with fewer possible transmissions by using fixed or limited
transport blocks compatible with the tiling SCHC fragmentation
handling. For SCHC fragmentation parameters see section [Section 4.3.2](#).

## 4.3. End-to-End Compression

The Non-IP Data Delivery (NIDD) services of 3GPP enable the
transmission of SCHC packets compressed by the application layer.
The packets can be delivered using IP-tunnels to the 3GPP network or
NGW-SCEF functions (i.e., API calls). In both cases, as compression
occurs before transmission, the network will not understand the
packet, and the network does not have context information of this
compression. Therefore the network will treat the packet as Non-IP
traffic and deliver it to the other side without any other protocol
stack element, directly under the L2.

### 4.3.1. SCHC Entities Placing

In the two scenarios using End-to-End compression, SCHC entities are
located almost on top of the stack. The NB-IoT connectivity services
implement SCHC in the Dev, an in the Application Server. The IP
tunneling scenario requires that the Application Server send the
compressed packet over an IP connection terminated by the 3GPP core
network. If the transmission uses the NGW-SCEF services, it is
possible to utilize an API call to transfer the SCHC packets between
the core network and the Application Server. Also, an IP tunnel
could be established by the Application Server if negotiated with
the NGW-SCEF.

```
+---------+           XXXXXXXXXXXXXXXXXXXXXXXX              +--------+
| SCHC    |      XXX                      XXX              | SCHC   |
|(Non-IP) +-----XX........................XX....+--*---+(Non-IP)|
+---------+    XX                +----+  XX   |  |   +--------+
|         |   XX                 |SCEF+-------+  |   |        |
|         |   XXX      3GPP RAN & +----+  XXX     +---+  UDP   |
|         |   XXX      CORE NETWORK     XXX      |  |          |
|   L2    +---+XX                +-----------+   |   +--------+
|         |     XX               |IP TUNNELING+--+   |        |
|         |      XXX             +-----------+  +---+   IP    |
+---------+      XXXX                XXXX       |   +--------+
| PHY     +------+ XXXXXXXXXXXXXXXXXXXXXXXX      +---+  PHY    |
+---------+                                       +--------+
   UE                                               AS
```
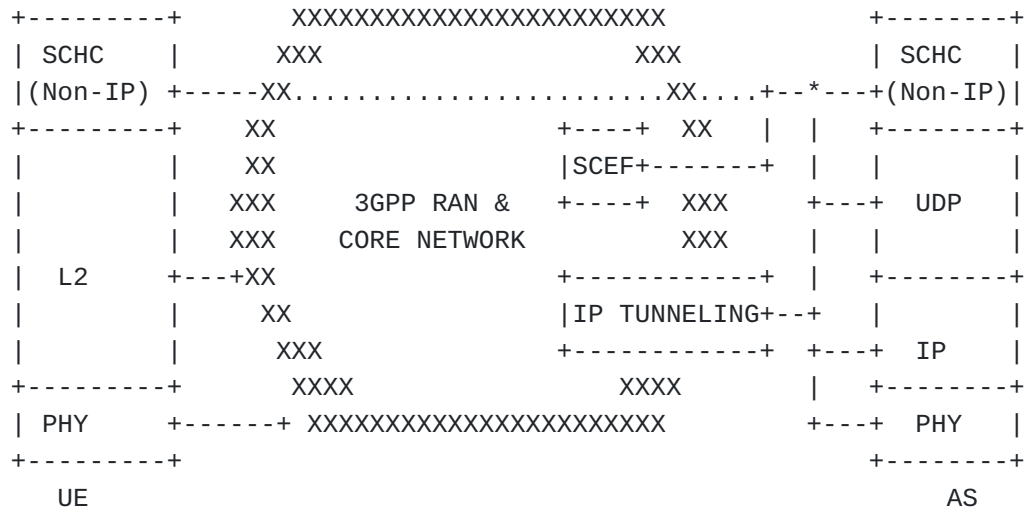
Figure 4: SCHC entities placed when using Non-IP Delivery (NIDD) 3GPP
                           Sevices

## 4.3.2.  Parameters for Static Context Header Compression and Fragmentation (SCHC)

These scenarios may use SCHC header compression capability to
improve the transmission of IPv6 packets. The use of SCHC for IoT
applications MUST be considered to enhance device connectivity.

  *SCHC Context initialization. The application layer handles the
   static context; consequently, the context distribution must be
   according to the application's capabilities, perhaps utilizing IP
   data transmissions up to context initialization. Also, the static
   contexts delivery may use the same IP tunneling or NGW-SCEF
   services used later for the SCHC packets transport.

  *SCHC Rules. Even when the transmission content is not visible for
   the 3GPP network, the same limitations as for Section 4.1 and
   Section 4.2 transmissions apply in these scenarios in terms of
   aiming to use the minimum number of transmissions and minimize
   the protocol overhead.

  *Rule ID Similar to the case of Section 4.1 and Section 4.2, these
   scenarios can dynamically set the RuleID size before the context
   delivery. For example, negotiate between the applications when
   choosing a profile according to the type of traffic and
   application deployed. The same considerations related to the
   transport block size and performance mentioned for the Section
   4.1 and Section 4.2 must be followed when choosing a size value
   for the RuleID field.

*SCHC MAX_PACKET_SIZE In these scenarios, the maximum recommended
    MTU size is 1358 Bytes since the SCHC packets (and fragments) are
    traversing the whole 3GPP network infrastructure (core and
    radio), not only the radio as the IP transmissions case.

   *Fragmentation Packets larger than 1358 bytes need the SCHC
    fragmentation function. Since the 3GPP uses reliability
    functions, the No-ACK fragmentation mode may be enough in point-
    to-point connections. Nevertheless, additional considerations are
    described below for more complex cases.

   *Fragmentation modes A global service assigns a QoS to the packets
    depending on the billing. Packets with very low QoS may get lost
    before arriving in the 3GPP radio network transmission, for
    example, in between the links of a capillarity gateway or due to
    buffer overflow handling in a backhaul connection. The use of
    SCHC fragmentation with the ACK-on-Error mode is recommended to
    secure additional reliability on the packets transmitted with a
    small trade-off on further transmissions to signal the end-to-end
    arrival of the packets if no transport protocol takes care of
    retransmission.
    Also, the ACK-on-Error mode is even desirable to keep track of
    all the SCHC packets delivered. In that case, the fragmentation
    function could be active for all packets transmitted by the
    applications. SCHC ACK-on-Error fragmentation may be active in
    transmitting non-IP packets on the NGW-MME. A non-IP packet will
    use SCHC reserved RuleID for non-compressing packets as [RFC8724]
    allows it.

   *Fragmentation Parameters SCHC profile will have specific Rules
    for the fragmentation modes. The rule will identify, which
    fragmentation mode is in use, and section Section 4.2.2 defines
    the RuleID size.

SCHC parametrization considers that NBIoT aligns the bit and uses
padding and the size of the Transfer Block. SCHC will try to reduce
padding to optimize the compression of the information. The Header
size needs to be multiple of 4, and the Tiles may keep a fixed value
of 4 or 8 bits to avoid padding except for transfer block equals 16
bits where Tiles may be 2 bits. The transfer block size has a wide
range of values. Two configurations are recommended for the
fragmentation parameters.

   *For Transfer Blocks smaller or equal to 304bits using an 8 bits-
    Header_size configuration, with the size of the header fields as
    follows:

       -RuleID from 1 - 3 bits,

-DTag 1 bit,

        -FCN 3 bits,

        -W 1 bits.

    *For Transfer Blocks bigger than 304 bits using a 16 bits-
     Header_size configuration, with the size of the header fields as
     follows:

        -RulesID from 8 - 10 bits,

        -DTag 1 or 2 bits,

        -FCN 3 bits,

        -W 2 or 3 bits.

        -W 2 or 3 bits.

    *WINDOW_SIZE is recommended to be 2^N-1.

    *RCS will follow the default size defined in section 8.2.3 of the
     [RFC8724], with a length equal to the L2 Word.

    *MAX_ACK_REQ is recommended to be 2, but applications may change
     this value based on transmission conditions.

   The IoT devices communicate with small data transfer and have a
   battery life of 10 years. These devices use the Power Save Mode and
   the Idle Mode DRX, which govern how often the device wakes up, stays
   up, and is reachable. Table 10.5.163a in {3GPP-TS_24.088} specifies
   a range for the radio timers as N to 3N in increments of one where
   the units of N can be 1 hour or 10 hours. The Inactivity Timer and
   the Retransmission Timer be set based on these limits.

5.  Padding

   NB-IoT and 3GPP wireless access, in general, assumes byte-aligned
   payload. Therefore the L2 word for NB-IoT MUST be considered 8 bits,
   and the padding treatment should use this value accordingly.

6.  IANA considerations

   This document has no IANA actions.

## 7.  Security considerations

This document does not add any security considerations and follows
the [RFC8724] and the 3GPP access security document specified in
[TR33203].

## 8.  Appendix

### 8.1.  NB-IoT User Plane protocol architecture

#### 8.1.1.  Packet Data Convergence Protocol (PDCP)

Each of the Radio Bearers (RB) is associated with one PDCP entity.
Moreover, a PDCP entity is associated with one or two RLC entities
depending on the unidirectional or bi-directional characteristics of
the RB and RLC mode used. A PDCP entity is associated with either a
control plane or a user plane with independent configuration and
functions. The maximum supported size for NB-IoT of a PDCP SDU is
1600 octets. The primary services and functions of the PDCP sublayer
for NB-IoT for the user plane include:

  *Header compression and decompression using ROHC (Robust Header
   Compression)

  *Transfer of user and control data to higher and lower layers

  *Duplicate detection of lower layer SDUs when re-establishing
   connection (when RLC with Acknowledge Mode in use for User Plane
   only)

  *Ciphering and deciphering

  *Timer-based SDU discard in uplink

#### 8.1.2.  Radio Link Protocol (RLC)

RLC is a layer-2 protocol that operates between the UE and the base
station (eNB). It supports the packet delivery from higher layers to
MAC, creating packets transmitted over the air, optimizing the
Transport Block utilization. RLC flow of data packets is
unidirectional, and it is composed of a transmitter located in the
transmission device and a receiver located in the destination
device. Therefore to configure bi-directional flows, two sets of
entities, one in each direction (downlink and uplink), must be
configured and effectively peered to each other. The peering allows
the transmission of control packets (ex., status reports) between

entities. RLC can be configured for data transfer in one of the
following modes:

  *Transparent Mode (TM). RLC does not segment or concatenate SDUs
   from higher layers in this mode and does not include any header
   to the payload. RLC receives SDUs from upper layers when acting
   as a transmitter and transmits directly to its flow RLC receiver
   via lower layers. Similarly, a TM RLC receiver would only deliver
   without processing the packets to higher layers upon reception.

  *Unacknowledged Mode (UM). This mode provides support for
   segmentation and concatenation of payload. The RLC packet's size
   depends on the indication given at a particular transmission
   opportunity by the lower layer (MAC) and is octets aligned. The
   packet delivery to the receiver does not include reliability
   support, and the loss of a segment from a packet means a complete
   packet loss. Also, in the case of lower layer retransmissions,
   there is no support for re-segmentation in case of change of the
   radio conditions triggering the selection of a smaller transport
   block. Additionally, it provides PDU duplication detection and
   discards, reordering of out-of-sequence, and loss detection.

  *Acknowledged Mode (AM). In addition to the same functions
   supported by UM, this mode also adds a moving windows-based
   reliability service on top of the lower layer services. It also
   supports re-segmentation, and it requires bidirectional
   communication to exchange acknowledgment reports called RLC
   Status Report and trigger retransmissions. This model also
   supports protocol error detection. The mode used depends on the
   operator configuration for the type of data to be transmitted.
   For example, data transmissions supporting mobility or requiring
   high reliability would be most likely configured using AM.
   Meanwhile, streaming and real-time data would be mapped to a UM
   configuration.

## 8.1.3.  Medium Access Control (MAC)

MAC provides a mapping between the higher layers abstraction called
Logical Channels comprised by the previously described protocols to
the Physical layer channels (transport channels). Additionally, MAC
may multiplex packets from different Logical Channels and prioritize
what to fit into one Transport Block if there is data and space
available to maximize data transmission efficiency. MAC also
provides error correction and reliability support through HARQ,
transport format selection, and scheduling information reporting
from the terminal to the network. MAC also adds the necessary
padding and piggyback control elements when possible and the higher
layers data.

```
                                     <Max. 1600 bytes>
                 +---+           +---+              +------+
Application      |AP1|           |AP1|              |  AP2 |
(IP/non-IP)      |PDU|           |PDU|              |  PDU |
                 +---+           +---+              +------+
                  |   |           |   |              |      |
PDCP         +--------+       +--------+       +-----------+
             |PDCP|AP1|       |PDCP|AP1|       |PDCP|  AP2 |
             |Head|PDU|       |Head|PDU|       |Head|  PDU |
             +--------+       +--------+       +--------+--\
              |   |   |   |    |   |   |        |    |   |\  `----\
         +---------------------------+    |    |(1)| `-----\(2)'-\
RLC      |RLC |PDCP|AP1|RLC |PDCP|AP1| +-------------+    +----|---+
         |Head|Head|PDU|Head|Head|PDU| |RLC |PDCP|AP2|    |RLC |AP2|
         +-------------|-------------+ |Head|Head|PDU|    |Head|PDU|
          |        |   |          |   | +---------|---+    +--------+
          |        |   | LCID1    |   | /         /   /   /         /
         /        /   /        _/  _// _/  _/    / LCID2   /
          |        |   |        |   | /     _/  _/    /       ___/
          |        |   |        |   | ||       |   |    /       /
     +---------------------------------------------+ +-----------+---+
MAC  |MAC|RLC|PDCP|AP1|RLC|PDCP|AP1|RLC|PDCP|AP2|  |MAC|RLC|AP2|Pad|
     |Hea|Hea|Hea |PDU|Hea|Hea |PDU|Hea|Hea |PDU|  |Hea|Hea|PDU|din|
     |der|der|der |   |der|der |   |der|der |   |  |der|der|   |g  |
     +---------------------------------------------+ +-----------+---+
                    TB1                                    TB2
```

Figure 5: Example of User Plane packet encapsulation for two transport
blocks

## 8.2.  NB-IoT Data over NAS (DoNAS)

The Access Stratum (AS) protocol stack used by DoNAS is somehow
particular. Since the security associations are not established yet
in the radio network, to reduce the protocol overhead, PDCP (Packet
Data Convergence Protocol) is bypassed until AS security is
activated. RLC (Radio Link Control protocol) uses by default the AM
mode, but depending on the network's features and the terminal, it
may change to other modes by the network operator. For example, the
transparent mode does not add any header or process the payload to
reduce the overhead, but the MTU would be limited by the transport
block used to transmit the data, which is a couple of thousand bits
maximum. If UM (only Release 15 compatible terminals) is used, the
RLC mechanisms of reliability are disabled, and only the reliability
provided by the MAC layer by Hybrid Automatic Repeat reQuest (HARQ)
is available. In this case, the protocol overhead might be smaller
than the AM case because of the lack of status reporting but with
the same support for segmentation up to 16000 Bytes. NAS packets are

encapsulated within an RRC (Radio Resource Control) TGPP36331 message.

Depending on the data type indication signaled (IP or non-IP data), the network allocates an IP address or establishes a direct forwarding path. DoNAS is regulated under rate control upon previous agreement, meaning that a maximum number of bits per unit of time is agreed upon per device subscription beforehand and configured in the device. The use of DoNAS is typically expected when a terminal in a power-saving state requires a short transmission and receiving an acknowledgment or short feedback from the network. Depending on the size of buffered data to transmit, the UE might be instructed to deploy the connected mode transmissions instead, limiting and controlling the DoNAS transmissions to predefined thresholds and a good resource optimization balance for the terminal the network. The support for mobility of DoNAS is present but produces additional overhead.

```
    +--------+   +--------+   +--------+
    |        |   |        |   |        |       +-----------------+
    |   UE   |   |  C-BS  |   | C-SGN  |       |Roaming Scenarios|
    +----|---+   +--------+   +--------+       |   +--------+    |
         |            |            |           |   |        |    |
    +----------------|------------|+           |   |  P-GW  |    |
    |        Attach                |           |   +--------+    |
    +-----------------------------+            |        |        |
         |            |            |           |        |        |
  +------|------------|--------+   |           |        |        |
  |RRC Connection Establishment|   |           |        |        |
  |with NAS PDU transmission   |   |           |        |        |
  |& Ack Rsp                   |   |           |        |        |
  +---------------------------+    |           |        |        |
         |            |            |           |        |        |
         |            |Initial UE  |           |        |        |
         |            |message     |           |        |        |
         |            |----------->|           |        |        |
         |            |            |           |        |        |
         |            | +--------------------+|           |        |
         |            | |Checks Integrity    ||           |        |
         |            | |protection, decrypts||           |        |
         |            | |data                ||           |        |
         |            | +--------------------+|           |        |
         |            |            |      Small data packet        |
         |            |            |-------------------------------->
         |            |            |      Small data packet        |
         |            |            |<-------------------------------
         |            | +----------|---------+ |        |        |
         |            | |Integrity protection,| |        |        |
         |            | |encrypts data       | |        |        |
         |            | +--------------------+ |        |        |
         |            |            |           |        |        |
         |            |Downlink NAS|           |        |        |
         |            |message     |           |        |        |
         |            |<-----------|           |        |        |
  +---------------------+          |           |        |        |
  |Small Data Delivery, |          |           |        |        |
  |RRC connection release|         |           |        |        |
  +---------------------+          |           |        |        |
                                               |        |        |
                                               |        |        |
                                               +-----------------+
```
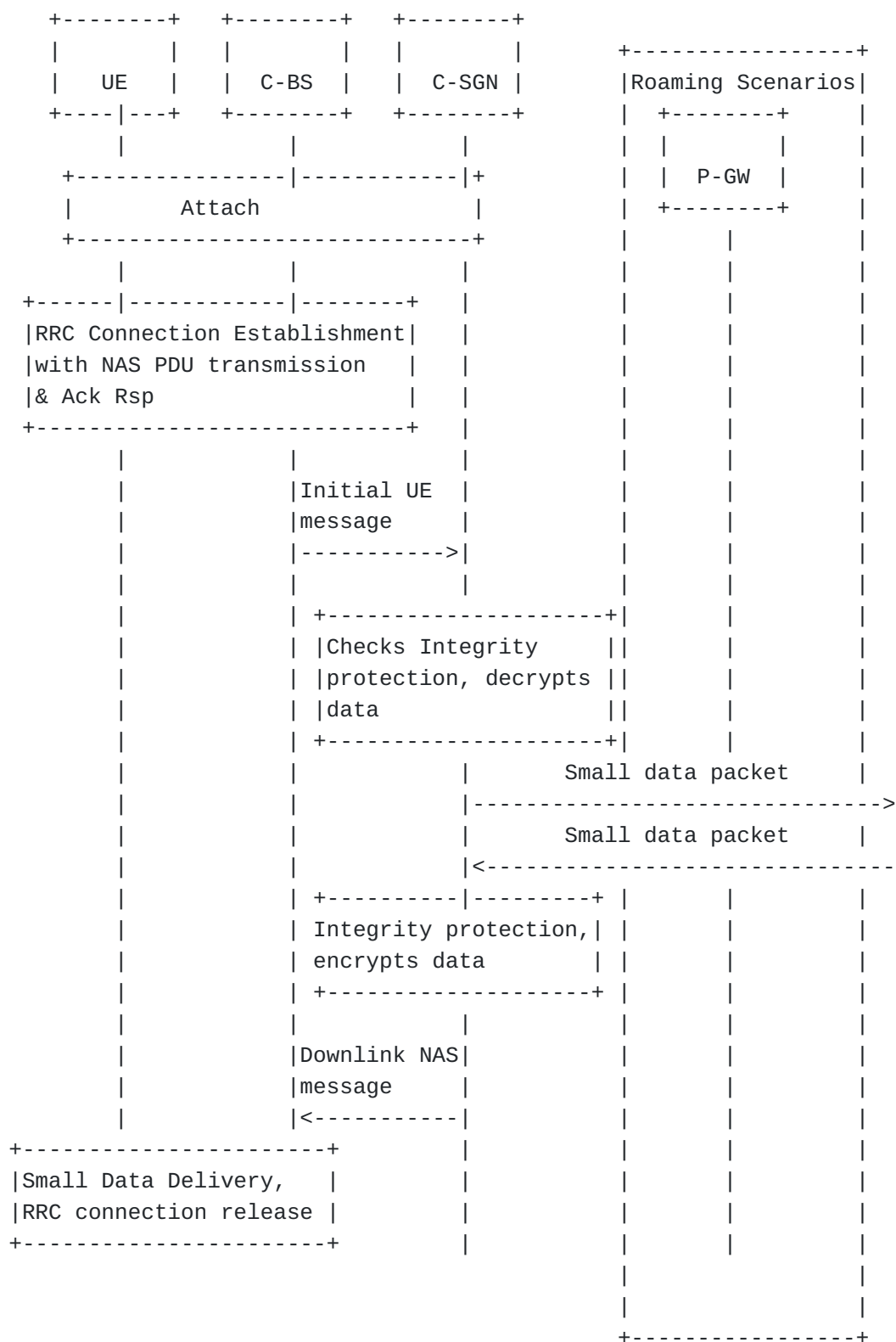
Figure 6: DoNAS transmission sequence from an Uplink initiated access

```
                    +---+ +---+ +---+                  +----+
 Application        |AP1| |AP1| |AP2|                  |AP2 |
 (IP/non-IP)        |PDU| |PDU| |PDU|  .............. |PDU |
                    +---+ +---+ +---+                  +----+
                     |   |/   /   |    \               |    |
 NAS /RRC       +--------+---|---+----+           +---------+
                |NAS/|AP1|AP1|AP2|NAS/|           |NAS/|AP2 |
                |RRC |PDU|PDU|PDU|RRC |           |RRC |PDU |
                +--------+-|-+---+----+           +---------|
                |         |\        |             |         |
                |<--Max. 1600 bytes-->|__          |_        |
                |          |  \__       \___        \_       \_
                |          |     \          \          \__     \_
        +---------------|+-----|----------+            \      \
 RLC    |RLC | NAS/RRC  ||RLC  | NAS/RRC  |      +----|-------+
        |Head|  PDU(1/2)||Head | PDU (2/2)|      |RLC |NAS/RRC|
        +---------------++---------------+      |Head|PDU    |
        |   |          | \            |         +------------+
        |   |   LCID1  |  \           |         |            /
        |   |          |   \          \         |            |
        |   |          |    \          \        |            |
        |   |          |     \          \    \   |
    +----+----+----------++-----|----+---------++----+---------|---+
 MAC |MAC |RLC |   RLC    ||MAC  |RLC |  RLC    ||MAC |  RLC    |Pad|
     |Head|Head|  PAYLOAD ||Head |Head| PAYLOAD ||Head|  PDU    |   |
     +----+----+----------++-----+----+---------++----+---------+---+
           TB1                   TB2                   TB3
```
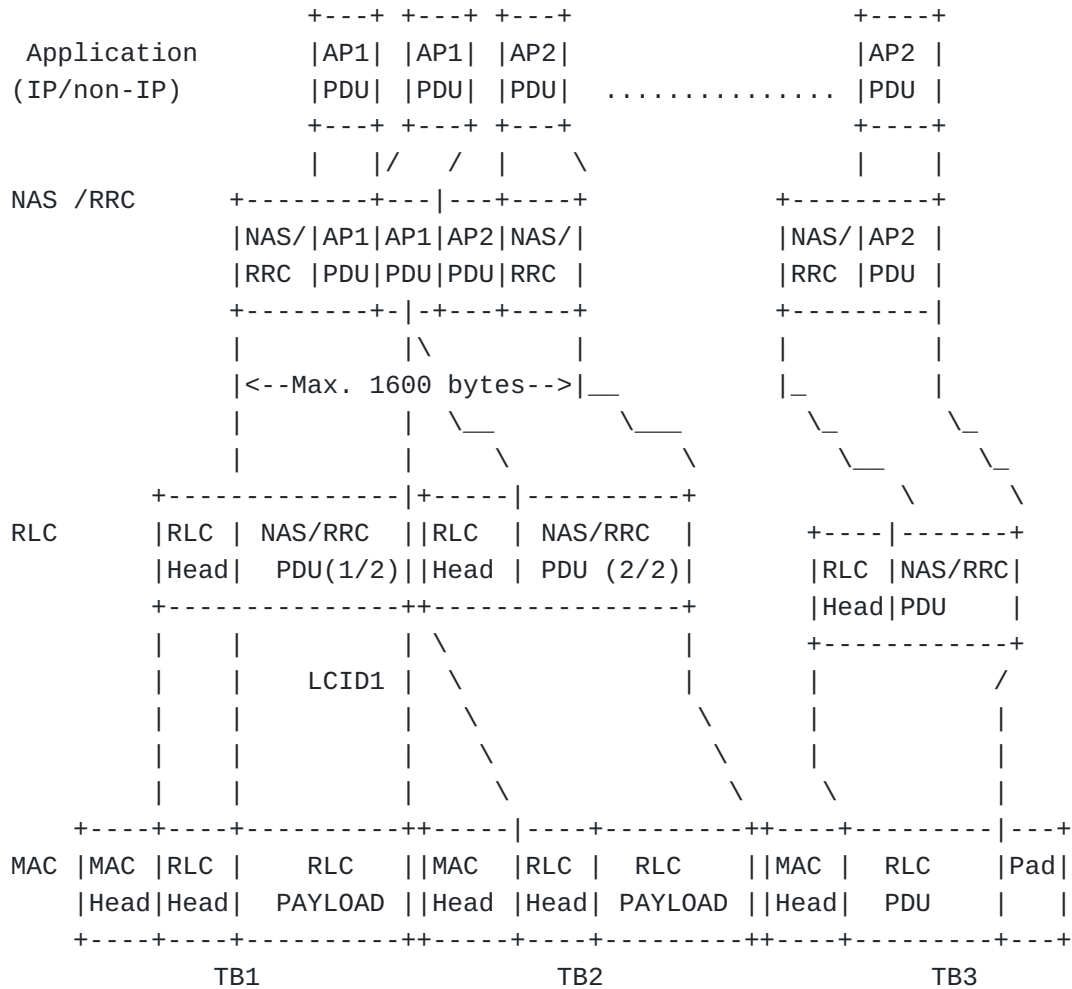
     Figure 7: Example of User Plane packet encapsulation for Data over NAS

## 9.  References

### 9.1.  Normative References

   [RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
              RFC2119, March 1997, <https://www.rfc-editor.org/info/
              rfc2119>.

   [RFC5795]  Sandlund, K., Pelletier, G., and L-E. Jonsson, "The
              RObust Header Compression (ROHC) Framework", RFC 5795,

DOI 10.17487/RFC5795, March 2010, <https://www.rfc-editor.org/info/rfc5795>.

[RFC8724]  Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/info/rfc8724>.

[TR23720]  3GPP, "Study on architecture enhancements for Cellular Internet of Things", 2015, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.720/23720-d00.zip>.

[TR24301]  3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification", 2016, <https://www.3gpp.org/ftp/Specs/archive/36_series/36.321/36321-d20.zip>.

[TR33203]  3GPP, "3G security; Access security fro IP-based services", 2015, <https://www.3gpp.org/ftp/Specs/archive/33_series/33.203/33203-d10.zip>.

[TR36321]  3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification", 2016, <https://www.3gpp.org/ftp/Specs/archive/36_series/36.321/36321-d20.zip>.

[TS36201]  3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description", 2018, <https://www.3gpp.org/ftp/Specs/archive/36_series/36.201/36201-f10.zip>.

[TS36322]  3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification", 2018, <https://www.3gpp.org/ftp/Specs/archive/36_series/36.322/36322-f01.zip>.

[TS36323]  3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification", 2016, <https://www.3gpp.org/ftp/Specs/archive/36_series/36.323/36323-d20.zip>.

[_3GPPR15] 3GPP, "The Mobile Broadband Standard", 2019, <https://www.3gpp.org/release-15>.

## 9.2.  Informative References

[RFC8376]  Farrell, S., Ed., "Low-Power Wide Area Network (LPWAN) Overview", RFC 8376, DOI 10.17487/RFC8376, May 2018, <https://www.rfc-editor.org/info/rfc8376>.

**Authors' Addresses**

Edgar Ramos
Ericsson
Hirsalantie 11
FI- 02420 Jorvas, Kirkkonummi
Finland

Email: edgar.ramos@ericsson.com

Ana Minaburo
Acklio
1137A Avenue des Champs Blancs
35510 Cesson-Sevigne Cedex
France

Email: ana@ackl.io