lpwan Working Group
Internet-Draft
Intended status: Informational
Expires: September 8, 2019

A. Minaburo
Acklio
E. Ramos
Ericsson
S. Shanmugalingam
Acklio

March 07, 2019

LPWAN Static Context Header Compression (SCHC) over NB-IoT
draft-minaburo-lpwan-nbiot-hc-02

Abstract

The Static Context Header Compression (SCHC) specification describes a header compression and fragmentation functionalities for LPWAN (Low Power Wide Area Networks) technologies. SCHC was designed to be adapted over any of the LPWAN technologies.

This document describes the use of SCHC over the NB-IoT wireless access, and provides elements for an 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 September 8, 2019.

Table of Contents

1. Introduction

The Static Context Header Compression (SCHC) [I-D.ietf-lpwan-ipv6-static-context-hc] defines a header compression scheme and fragmentation functionality, both specially tailored for Low Power Wide Area Networks (LPWAN) networks defined in [RFC8376].

Header compression is needed to efficiently bring Internet connectivity to the node within an NB-IoT network. SCHC uses a static context to performs header compression with specific parameters that need to be adapted into the NB-IoT wireless access. This document assumes functionality for NB-IoT of 3GPP release 15 otherwise other versions functionality is explicitly mentioned in the text.

This document describes the use of SCHC and its parameterizing over the NB-IoT wireless access.

2. Terminology

This document will follow the terms defined in [I-D.ietf-lpwan-ipv6-static-context-hc], in [RFC8376], and the [TGPP23720].

- CIoT. Cellular IoT
- C-SGN. CIoT Serving Gateway Node
- UE. User Equipment
- eNB. 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 network from LTE based systems.

- MME. Mobility Management Entity. Handle mobility of the UE

- NB-IoT. Narrow Band IoT. Referring to 3GPP LPWAN technology based in LTE architecture but with additional optimization for IoT and using a Narrow Band spectrum frequency.

- SGW. Serving Gateway. Routes and forwards the user data packets through the access network

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

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

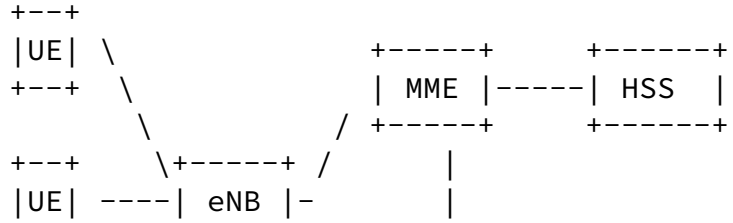
- PDU. Protocol Data Unit. Data packets including headers that are transmitted between entities through a protocol.

- SDU. Service Data Unit. Data packets (PDUs) from higher layers protocols used by lower layer protocols as a payload of their own PDUs that has not yet been encapsulated.

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

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

3. Architecture



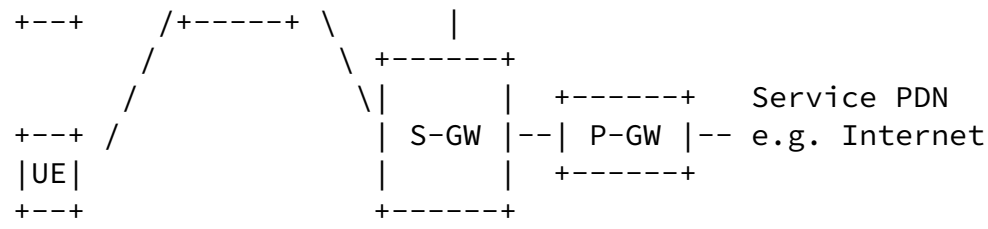


Figure 1: 3GPP network architecture

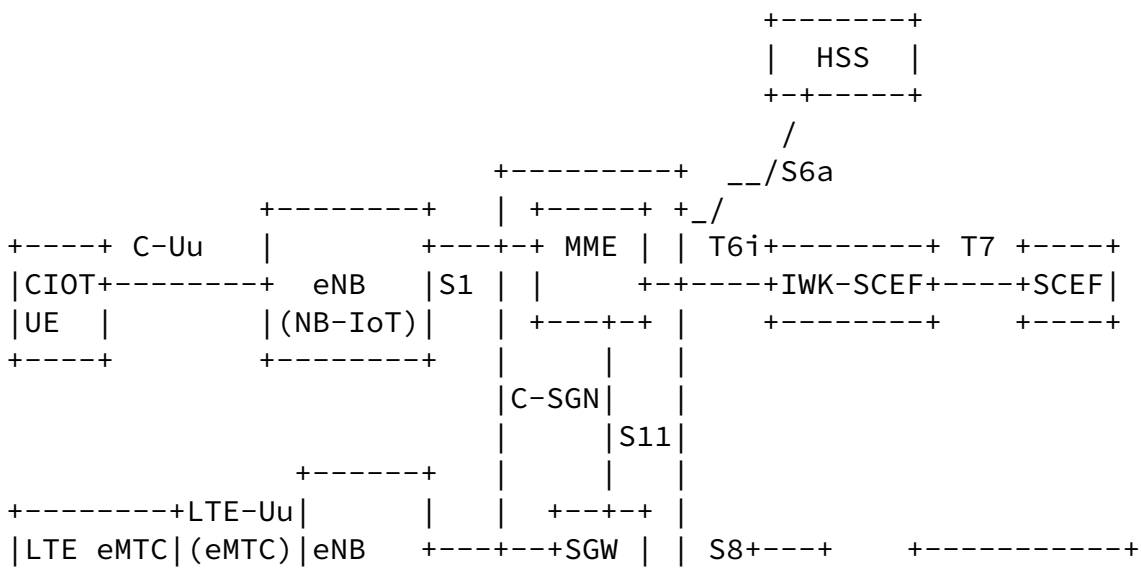
The architecture for 3GPP LTE network has been reused for NB-IoT with some optimizations and simplifications known as Cellular IoT (CIoT). Considering the typical use cases for CIoT devices here are described some of the additions to the LTE architecture specific for CIoT. C-SGN(CIoT Serving Gateway Node) is a deployment option co-locating EPS entities in the control plane and user plane paths (for example, MME + SGW + P-GW) and the external interfaces of the entities supported. The C-SGN also supports at least some of the following CIoT EPS Optimizations:

- o Control Plane CIoT EPS Optimization for small data transmission.
- o User Plane CIoT EPS Optimization for small data transmission.
- o Necessary security procedures for efficient small data transmission.
- o SMS without combined attach for NB-IoT only UEs.
- o Paging optimizations for coverage enhancements.
- o Support for non-IP data transmission via SGi tunneling and/or SCEF.
- o Support for Attach without PDN (Packet Data Network) connectivity.

Another node introduced in the CIOT architecture is the SCEF (Service Capability Exposure Function) that provide means to securely expose service and network capabilities to entities external to the network operator. The northbound APIS are defined by OMA and OneM2M. The main functions of a SCEF are:

- Non-IP Data Delivery (NIDD) established through the SCEF.

- Monitoring and exposure of event related to UE reachability, loss of connectivity, location reporting, roaming status, communication failure and change of IMEI-IMSI association.



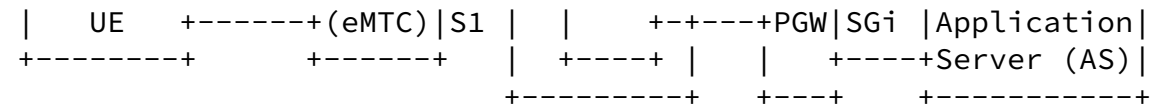


Figure 2: 3GPP optimized CIOT network architecture

4. Data Transmission

3GPP networks deal not only with data transmitted end-to-end but also with in-band signaling that is used between the nodes and functions to configure, control and monitor the system functions and behaviors. The control data is handled using a Control Plane which has a specific set of protocols, handling processes and entities. In contrast, the end-to-end or user data utilize a User Plane with characteristics of its own separated from the Control Plane. The handling and setup of the Control Plane and User Plane spans over the whole 3GPP network and it has particular implications in the radio network (i.e., EUTRAN) and in the packet core (ex., EPC).

For the CIOT cases, additionally to transmissions of data over User Plane, 3GPP has specified optimizations for small data transmissions, allowing to transport user data (IP, Non-IP) within signaling on the access network (Data transmission over Control Plane or Data Over NAS).

The maximum recommended MTU size is 1358 Bytes. The radio network protocols limit the packet sizes to be transmitted over the air including radio protocol overhead to 1600 Octets. But the value is reduced further to avoid fragmentation in the backbone of the network due to the payload encryption size (multiple of 16) and handling of the additional core transport overhead.

NB-IoT and in general the cellular technologies interfaces and functions are standardized by 3GPP. Therefore the introduction of SCHC entities to UE, eNB and C-SGN does need to be specified in the NB-IoT standard. This implies that standard specified SCHC support would not be backwards compatible. A terminal or a network supporting a version of the standard without support of SCHC or without capability implementation (in case of not being standardized as mandatory capability) is not able to utilize the compression

services with this approach.

SCHC could be deployed differently depending on where the header compression and the fragmentation are applied. The SCHC functionalities could be applied to the packets about to be transmitted over the air, or to the whole end-to-end link. To accomplish the first, it is required to place SCHC compression and decompression entities in the eNB and in the UE for transmissions over the User Plane. Additionally, to handle the case of the transmissions over Control Plane or Data Over NAS, the network SCHC entity has to be placed in the C-SGN as well. For these two cases, the functions are 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. In that case, the SCHC entities would be placed in the application layer of the terminal in one end, and either in the application servers or in a broker function in the edge of the operator network in the other end. For the radio network, the packets are transmitted as non-IP traffic, which can be currently served utilizing 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 utilizing the non-IP transmission features of the operator network.

Accordingly, there are four different scenarios where SCHC can be used in the NB-IoT architecture. IP header compression on the data transmission over User Plane, IP header compression on the optimized transmissions over Control Plane (i.e.,DoNAS), non-IP transmissions of SCHC packets by IP tunneling, and non-IP transmissions of SCHC packets by SCEF forwarding. The following sections describe each of them in more detail. The first two scenarios refer to transmissions using the 3GPP IP transmission capabilities and the last two refers to transmission using the Non-IP capabilities.

5. IP based Data Transmission

5.1. SCHC over User Plane transmissions

Deploying SCHC only over the radio link would require to place it as part of the User Plane data transmission. The User Plane utilizes the protocol stack of the Access Stratum (AS) for data transfer. AS (Access Stratum) is the functional layer responsible for transporting data over wireless connection and managing radio resources. The user plane AS has support for features such as reliability, segmentation and concatenation. The transmissions of the AS make use of link adaptation, meaning that the transport format utilized for the transmissions are optimized according to the radio conditions, the number of bits to transmit and the power and interference constrains. That means that the number of bits transmitted over the air depends of the Modulation and Coding Schemes (MCS) selected. The transmissions in the physical layer happens at network synchronized intervals of times called TTI (Transmission Time Interval). The transmission of a Transport Block (TB) is completed during, at least, one TTI. Each Transport Block has a different MCS and number of bits available to transmit. The Transport Blocks characteristics are defined by the MAC technical specification [TGPP36321]. The Access Stratum for User Plane is comprised by Packet Data Convergence Protocol (PDCP) [TGPP36323], Radio Link Protocol (RLC)[TGPP36322], Medium Access Control protocol (MAC)[TGPP36321] and the Physical Layer [TGPP36201]. More details of this protocols are given in the Appendix.

5.1.1. SCHC Entities Placing

The current architecture provides support for header compression in PDCP utilizing RoHC [RFC5795]. Therefore SCHC entities can be deployed in similar fashion without need for major changes in the 3GPP specifications.

In this scenario, RLC takes care of the handling of fragmentation (if transparent mode is not configured) when packets exceeds the transport block size at the time of transmission. Therefore SCHC fragmentation is not needed and should not be used to avoid additional protocol overhead. It is not common to configure RLC in Transparent Mode for IP based user plane data. But 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.

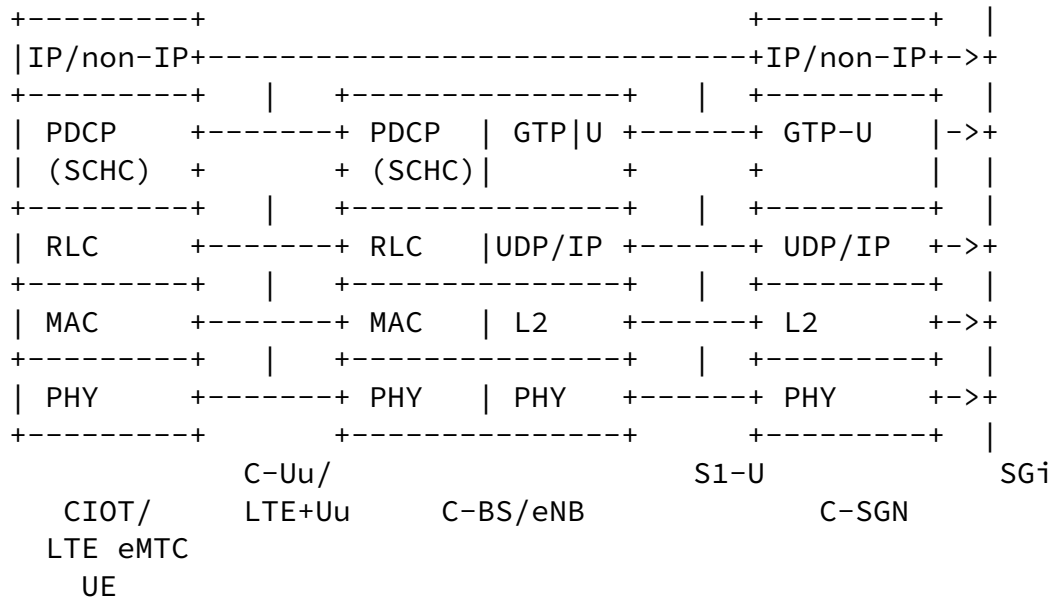


Figure 3: SCHC entities placement in the 3GPP CIOT radio protocol architecture for data over user plane

5.2. Data Over Control Plane

The Non-Access Stratum (NAS), conveys mainly control signaling between the UE and the cellular network [TGPP24301]. NAS is transported on top of the Access Stratum (AS) already mentioned in the previous section.

NAS has been adapted to provide support for user plane data transmissions to reduce the overhead when transmitting infrequent small quantities of data. This is known as Data over NAS (DoNAS) or Control Plane CIoT EPS optimization. In DoNAS the UE makes use of the pre-established NAS security and piggyback uplink small data into the initial NAS uplink message, and uses an additional NAS message to receive downlink small data response.

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

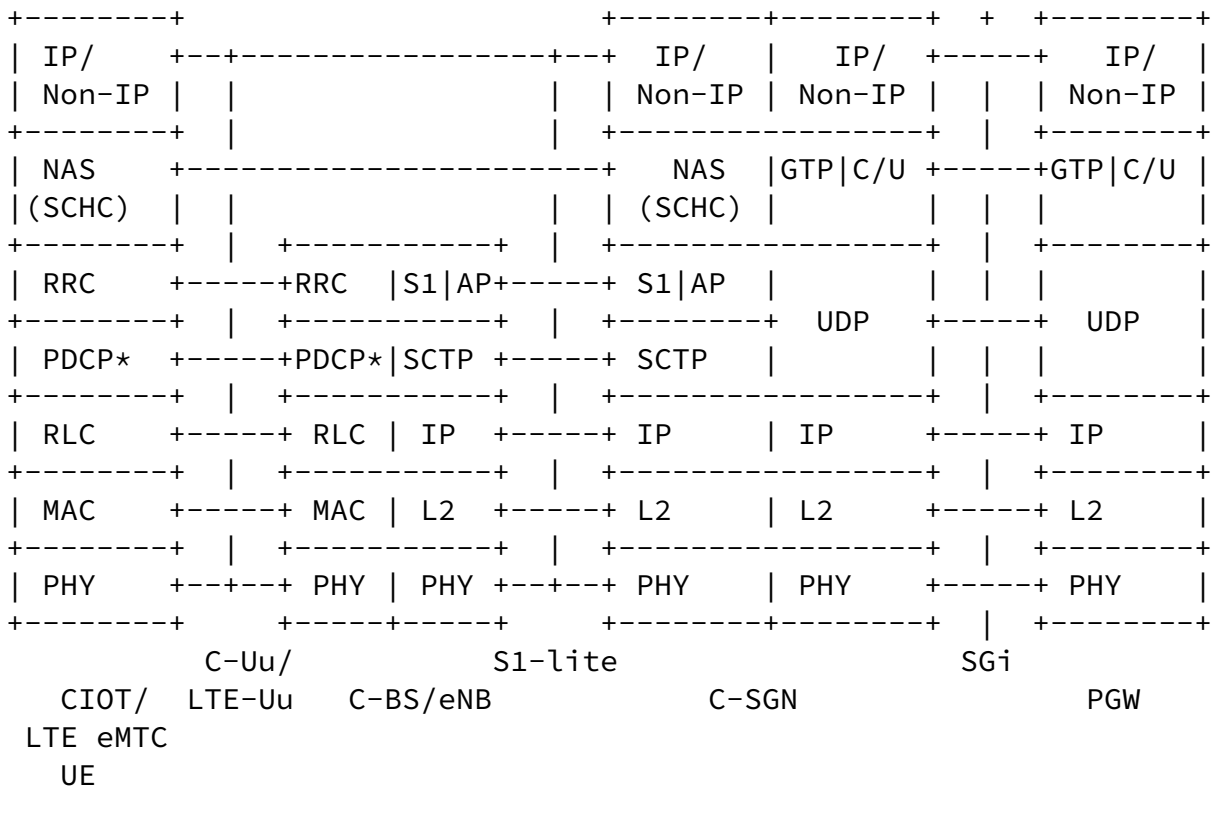
The use of DoNAS is typically expected when a terminal in a power saving state requires to do a short transmission and receive an

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 and the network. The support for mobility of DoNAS is present but produces additional overhead. Additional details of DoNAS are given in the Appendix.

5.2.1. SCHC Entities Placing

In this scenario SCHC can be applied in the NAS protocol layer instead of PDCP. The same principles than for user plane transmissions applies here as well. The main difference is the physical placing of the SCHC entities in the network side as the C-SGN (placed in the core network) is the terminating node for NAS instead of the eNB.



*PDCP is bypassed until AS security is activated [TGPP36300].

Figure 4

5.3. Parameters for Static Context Header Compression (SCHC)

5.3.1. SCHC Context initialization

RRC (Radio Resource Control) protocol is the main tool used to configure the operation parameters of the AS transmissions for 3GPP technologies. RoHC operation is configured with this protocol and it is to expect that SCHC will be configured and the static context distributed in similar fashion for these scenarios.

5.3.2. SCHC Rules

The number of rules in a context are defined by the network operator in these scenarios. For this, the operator must be aware of the type of IP traffic that the device will carry out. This means that the operator might provision sets of rules compatible with the use case of the device. For devices acting as gateways of other devices several rules that match the diversity of devices and protocols used by the devices associated to the gateway. Meanwhile than simpler devices (for example an electricity meter) may have a predetermined set of protocols and parameters fixed. Additionally, the deployment of IPV4 addresses in addition to IPV6 may force to provision separate rules to deal with each of the cases.

5.3.3. Rule ID

For these transmission scenarios in NB-IoT, a reasonable assumption of 9 bytes of radio protocol overhead can be expected. PDCP 5 bytes due to header and integrity protection, and 4 bytes of RLC and MAC. The minimum physical Transport Block (TB) that can withhold this overhead value according to 3GPP Release 15 specifications are: 88, 104, 120 and 144 bits. If it is wished to optimize the number of transmissions of a very small application packet so that in some cases can be transmitted using only one physical layer transmission,

then the SCHC overhead should not exceed the available number of bits of the smallest utile physical TB available. The packets handled by 3GPP networks are byte-aligned, and therefore the minimum payload possible (including padding) is 8 bits. Therefore in order to utilize the smallest TB the maximum SCHC is 8 bits. This must include the Compression Residue in addition to the Rule ID. In the other hand, it is possible that more complex NB-IoT devices (such as a capillarity gateway) might require additional bits to handle the variety and multiple parameters the 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 a configurable value is preferred for these scenarios. The configuration may be set as part of the operation profile agreed together with the context distribution. The Rule Id field size may range for example from 2 bits resulting in 4 rules to a 8 bits value that would yield up to 256 rules which can be

used together with the operators and seems quite a reasonable maximum limit even for a device acting as a NAT. More bits could be configured, but it should take in account the byte-alignment of the expected Compression Residue too. In the minimum TB size case, 2 bits size of Rule Id leave only 6 bits available for Compression Residue.

5.3.4. SCHC MAX_PACKET_SIZE

The Access Stratum can handle the fragmentation of SCHC packets if needed including reliability. Hence the packet size is limited by the MTU possible to be handled by the AS radio protocols that corresponds to 1600 bytes for 3GPP Release 15.

5.3.5. Fragmentation

For these scenarios the SCHC fragmentation functions are recommend to be 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 selection of the blocks is done according to the input of the link adaptation 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 depends of the network load, interference and number of bits to be transmitted and

QoS. Even if setting a value that allows the construction of data units following SCHC tiles principle, the protocol overhead may be greater or equal than allowing the AS radio protocols to take care of the fragmentation natively.

5.3.5.1. Fragmentation in Transparent Mode

If RLC is configured to operate 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 very rare to transmit user plane data using this configuration and it is mainly targeting control plane transmissions. In those cases the reliability is normally ensured by MAC based mechanisms, such as repetitions or automatic retransmissions, and additional reliability might only generate protocol overhead.

In future operations, it could be devised the utilization of SCHC to reduce radio network protocols overhead and support the reliability of the transmissions, and targeting small data with the fewer possible transmissions. This could be realized by using fixed or limited set of transport blocks compatible with the tiling SCHC fragmentation handling.

6. Non-IP based Data Transmission

The Non-IP Data Delivery (NIDD) services of 3GPP enable the possibility of transmitting SCHC packets compressed by the application layer. The packets can be delivered by means of IP-tunnels to the 3GPP network or using SCEF functions (i.e., API calls). In both cases the packet IP is not understood by the 3GPP network since it is already compressed and the network does not has information of the context used for compression. Therefore the network will treat the packet as a Non-IP traffic and deliver it to the UE without any other stack element, directly under the L2.

6.1. SCHC Entities Placing

In the two scenarios using NIDD, SCHC entities are located almost in top of the stack. In the terminal, it may be implemented by a application utilizing the NB-IoT connectivity services. In the network side, the SCHC entities are located in the Application Server

(AS). The IP tunneling scenario requires that the Application Server sends the compressed packet over an IP connection that is terminated by the 3GPP core network. If instead the SCEF services are used, then it is possible to utilize a API call to transfer the SCHC packets between the core network and the AS, also an IP tunnel could be established by the AS, if negotiated with the SCEF.

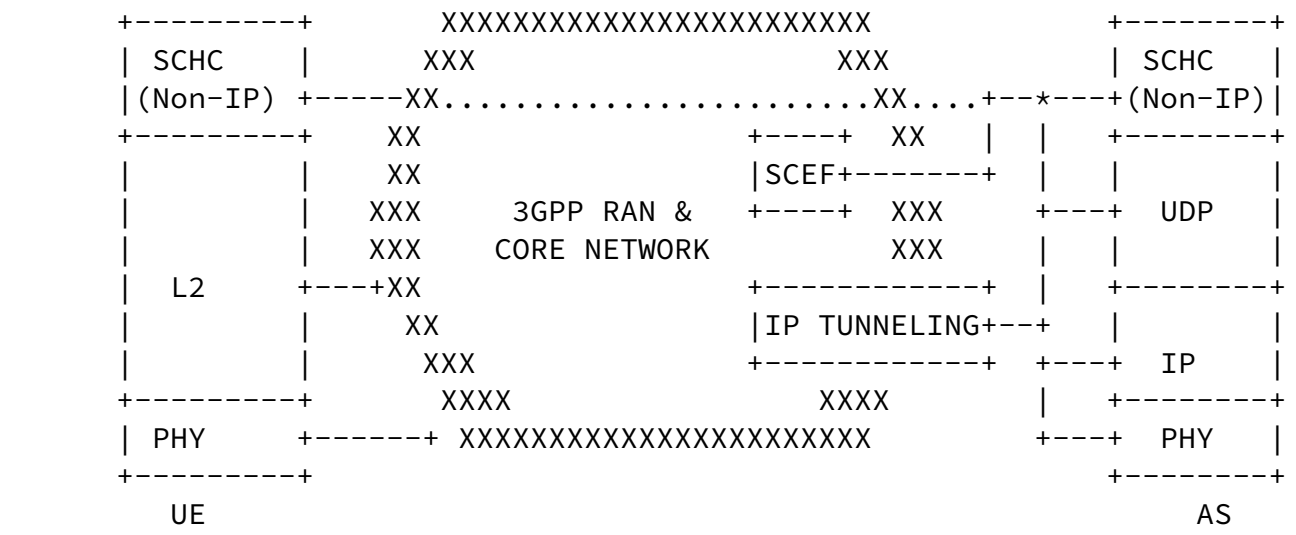


Figure 5: SCHC entities placed when using Non-IP Delivery (NIDD) 3GPP Sevices

6.2. Parameters for Static Context Header Compression

6.2.1. SCHC Context initialization

The static context is handled in the application layer level, consequently the contexts are required to be distributed according to the applications own capabilities, perhaps utilizing IP data transmissions up to context initialization. Also the same IP tunneling or SCEF services used later for the SCHC packets transport may be used by the applications in both ends to deliver the static contexts to be used.

6.2.2. SCHC Rules

Even when the transmissions content are not visible for the 3GPP network, the same limitations than for IP based data transmissions applies in these scenarios in terms of aiming to use the minimum number of transmission and minimize the protocol overhead.

6.2.3. Rule ID

Similarly to the case of IP transmissions, the Rule ID size can be dynamically set prior the context delivery. For example negotiated between the applications when choosing a profile according to the type of traffic and type of application deployed. Same considerations related to the transport block size and performance mentioned for the IP type of traffic has to be follow when choosing a size value for the Rule ID field.

6.2.4. SCHC MAX_PACKET_SIZE

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

6.3. Fragmentation

In principle the fragmentation function should be activated for packets greater than 1358 Bytes. Since the 3GPP reliability functions take great deal care of it, for simple point to point connections may be enough a NO-ACK mode. Nevertheless additional considerations for more complex cases are mentioned in the next subsection to be taken in account.

6.3.1. Fragmentation modes

Depending of the QoS that has been assigned to the packets, it is possible that packets are lost before they arrive to 3GPP radio

network transmission, for example in between the links of a capillarity gateway, or due to buffer overflow handling in a backhaul connection. In consequence, it is possible to secure additional reliability on the packets transmitted with a small trade-off on additional transmissions to signal the packets arrival indication end-to-end if no transport protocol takes care of retransmission. To achieve this, the packets fragmentation is activated with the ACK-on-Error mode enabled. In some cases, it 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 MAX_PACKET_SIZE == 1 Byte) and the ACK-on-Error mode.

6.3.2. Fragmentation Parameters(TBD)

- Rule ID
- DTag
- FCN
- W (number of bits)
- WINDOW_SIZE
- Retransmission Timer
- Inactivity Timer
- MAX_ACK_Retries
- MAX_ATTEMPS
- MIC (size and algorithm)

7. 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 treatment of padding should use this value accordingly.

8. Security considerations

3GPP access security is specified in (TGPP33203).

9. 3GPP References

- [TGPP23720] 3GPP, "TR 23.720 v13.0.0 - Study on architecture enhancements for Cellular Internet of Things", 2016.

- [TGPP33203] 3GPP, "TS 33.203 v13.1.0 - 3G security; Access security for IP-based services", 2016.

- [TGPP36321] 3GPP, "TS 36.321 v13.2.0 - Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification", 2016

- [TGPP36323] 3GPP, "TS 36.323 v13.2.0 - Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification", 2016.

- [TGPP36331] 3GPP, "TS 36.331 v13.2.0 - Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification", 2016.

- [TGPP36300] 3GPP, "TS 36.300 v15.1.0 - Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2", 2018

- [TGPP24301] 3GPP "TS 24.301 v15.2.0 - Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3", 2018

10. Appendix

10.1. NB-IoT User Plane protocol architecture

10.1.1. Packet Data Convergence Protocol (PDCP)

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

- Header compression and decompression by means of 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

10.1.2. 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 that are 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 set of entities, one in each direction (downlink and uplink) must be configured and they are 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). In this mode RLC do not segment or concatenate SDUs from higher layers and do not include any header to the payload. When acting as a transmitter, RLC receives SDUs from upper layers and transmit directly to its flow RLC receiver via lower layers. Similarly, an TM RLC receiver would only deliver without additional processing the packets to higher layers upon reception.
- Unacknowledged Mode (UM). This mode provides support for segmentation and concatenation of payload. The size of the RLC packet depends of the indication given at a particular transmission opportunity by the lower layer (MAC) and are octets

aligned. The packet delivery to the receiver do not include support for reliability and the lost of a segment from a packet means a whole packet loss. Also in 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 discard, reordering of out of sequence and loss detection.

- Acknowledged Mode (AM). Additional to the same functions supported from UM, this mode also adds a moving windows based reliability service on top of the lower layer services. It also provides support for re-segmentation and it requires bidirectional communication to exchange acknowledgment reports called RLC Status Report and trigger retransmissions is needed. Protocol error detection is also supported by this mode. The mode uses depends of 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 map to a UM configuration.

10.1.3. 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 the efficiency of data transmission. MAC also provides error correction and reliability support by means of 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 additional to the higher layers data.

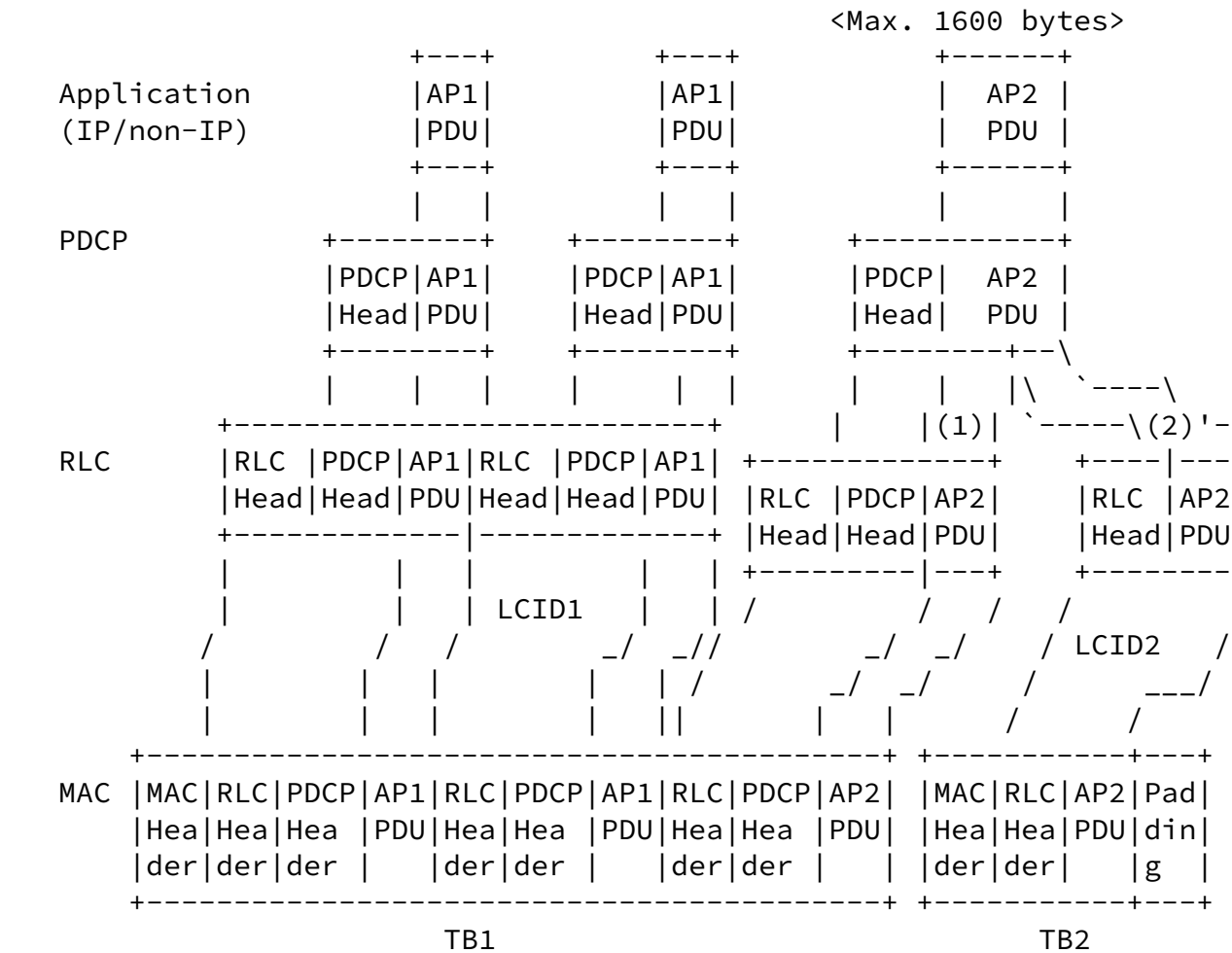

<Max. 1600 bytes>
Application
(IP/non-IP)
PDCP
RLC
MAC
LCID1
LCID2
TB1
TB2

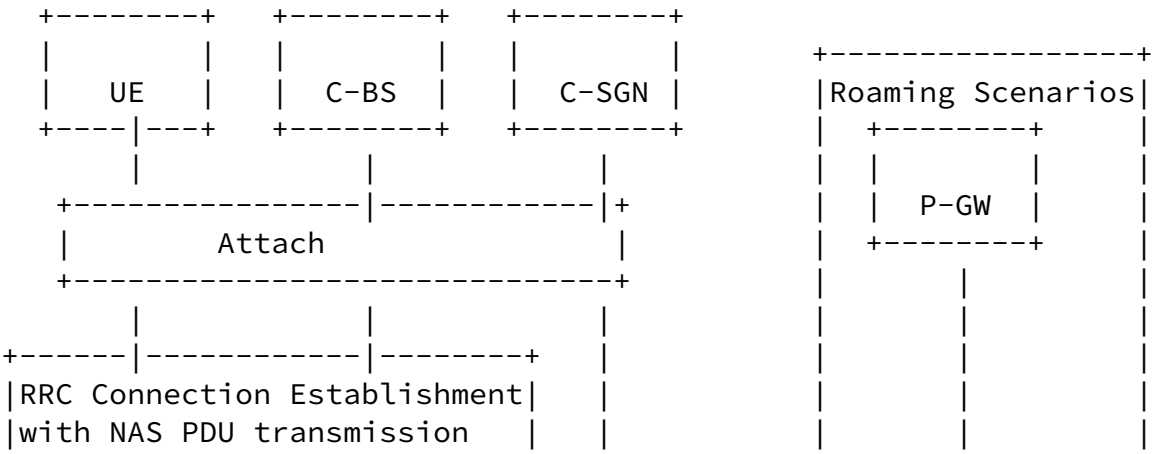
Figure 6: Example of User Plane packet encapsulation for two transport blocks

10.2. NB-IoT Data over NAS (DoNAS)

The AS protocol stack used by DoNAS is somehow special. 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) is configured by default in AM mode, but depending of the features supported by the network and the terminal it may be configured in other modes by the network operator. For example, the transparent mode does not add any header or does not process the payload in any way reducing the overhead, but the MTU would be limited by the transport block used to transmit the data which is couple of thousand of bits maximum. If UM (only Release 15 compatible terminals) is used, the RLC mechanisms of reliability is 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 for the AM case because the

lack of status reporting but with the same support for segmentation up to 16000 Bytes. NAS packet are encapsulated within a RRC (Radio Resource Control)[TGPP36331] message.

Depending of the data type indication signaled (IP or non-IP data), the network allocates an IP address or just establish 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 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 to do a short transmission and receive an acknowledgment or short feedback from the network. Depending of 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 and 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

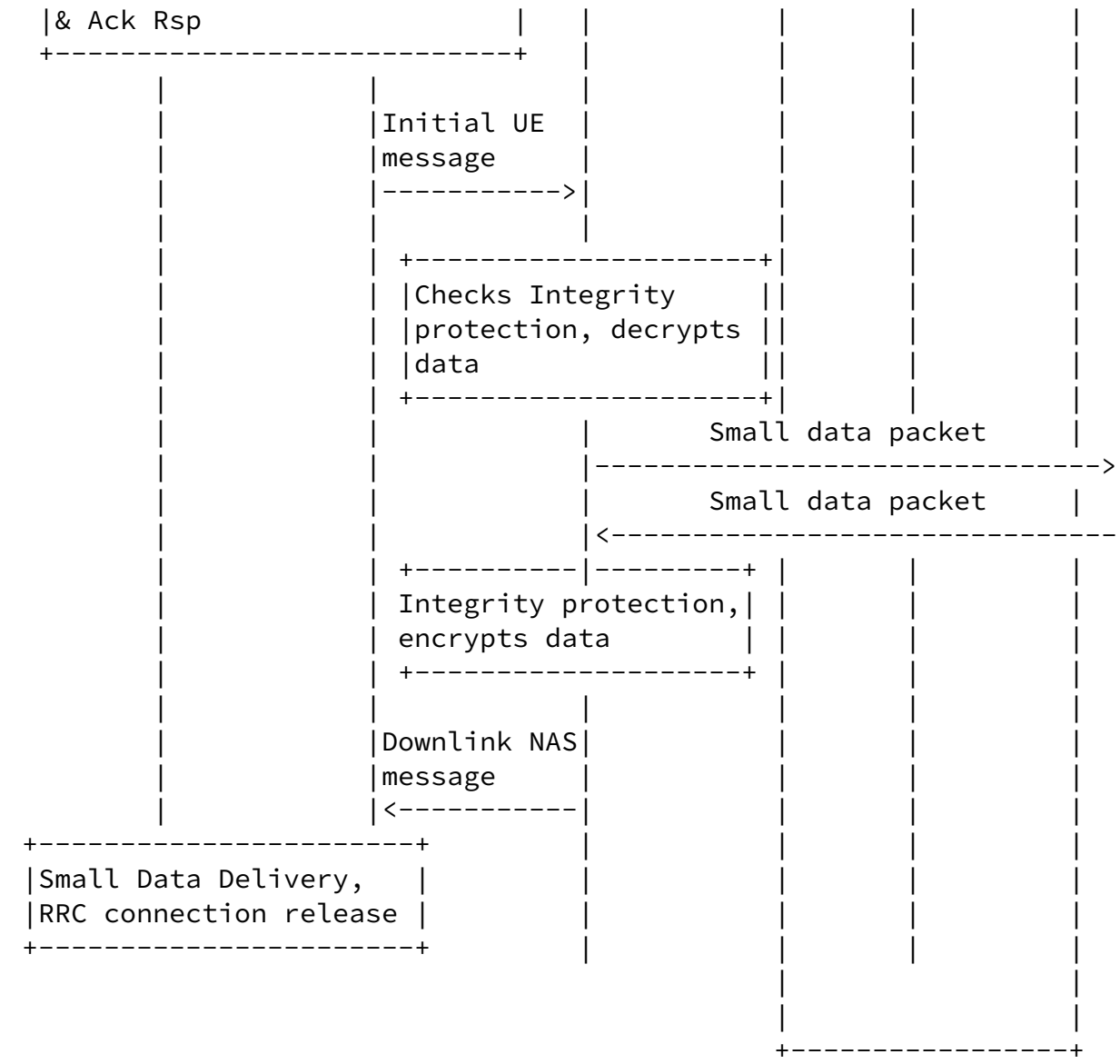
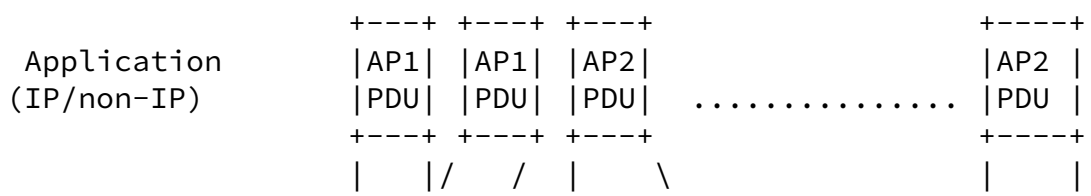


Figure 7: DoNAS transmission sequence from an Uplink initiated access



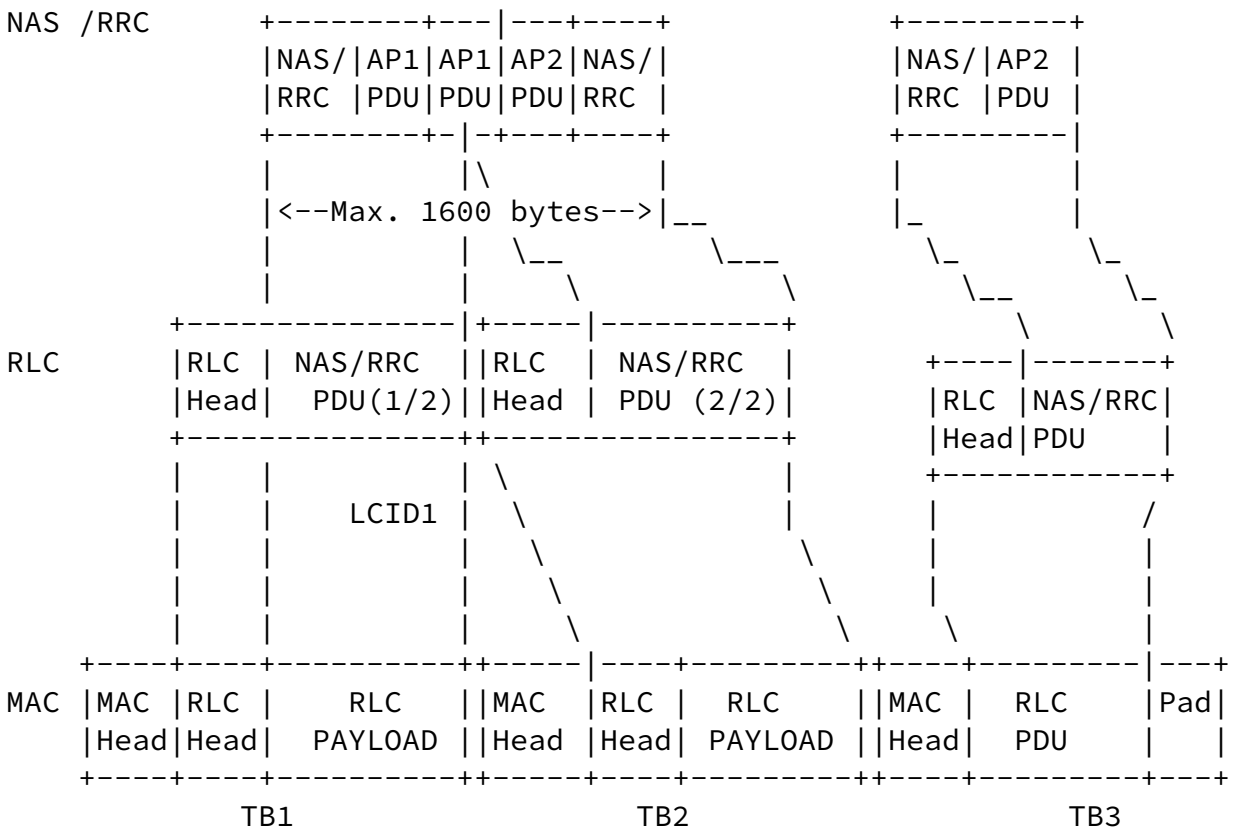


Figure 8: Example of User Plane packet encapsulation for Data over NAS

11. Informative References

[I-D.ietf-lpwan-ipv6-static-context-hc]
Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and J. Zuniga, "LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP", draft-ietf-lpwan-ipv6-static-context-hc-18 (work in progress), December 2018.

[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>.

[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

Ana Minaburo
Acklio
2bis rue de la Chataigneraie
35510 Cesson-Sevigne Cedex
France

Email: ana@ackl.io

Edgar Ramos
Ericsson
Hirsalantie 11
02420 Jorvas, Kirkkonummi
Finland

Email: edgar.ramos@ericsson.com

Sivasothy Shanmugalingam
Acklio
2bis rue de la Chataigneraie
35510 Cesson-Sevigne Cedex
France

Email: sothy@ackl.io