Workgroup: lpwan Working Group
Internet-Draft:
draft-ietf-lpwan-schc-over-nbiot-15
Published: 15 December 2022
Intended Status: Standards Track
Expires: 18 June 2023
Authors: E. Ramos A. Minaburo
Ericsson Acklio

Static Context Header Compression over Narrowband Internet of Things

Abstract

This document describes Static Context Header Compression and Fragmentation (SCHC) specifications, RFC 8724 and RFC 8824, combination with the 3rd Generation Partnership Project (3GPP) and the Narrowband Internet of Things (NB-IoT).

This document has two parts. One normative to specify the use of SCHC over NB-IoT. And one informational, which recommends some values if 3GPP wanted to use SCHC inside their architectures.

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 18 June 2023.

Table of Contents

1. Introduction

This document defines the scenarios where the Static Context Header Compression and fragmentation (SCHC) [RFC8724] and [RFC8824] are suitable for 3rd Generation Partnership Project (3GPP) and Narrowband Internet of Things (NB-IoT) protocol stacks.

In the 3GPP and the NB-IoT networks, header compression efficiently brings Internet connectivity to the Device-User Equipment (Dev-UE), the radio (RGW-eNB) and network (NGW-MME) gateways, and the Application Server. This document describes the SCHC parameters supporting static context header compression and fragmentation over the NB-IoT architecture.

This document assumes functionality for NB-IoT of 3GPP release 15 [_3GPPR15]. Otherwise, the text explicitly mentions other versions' functionality.

This document has two parts, a standard end-to-end scenario describing how any application must use SCHC over the 3GPP public service. And informational scenarios about how 3GPP could use SCHC in their protocol stack network.

2. Conventions and Definitions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminology

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

*Capillary Gateway. A capillary gateway facilitates seamless integration because it has wide area connectivity through cellular and provides wide area access as a proxy to other devices using LAN technologies (BT, Wi-Fi, Zigbee, or others.)

*CIoT EPS. Cellular IoT Evolved Packet System. It is a functionality to improve the support of small data transfers.

*Dev-UE. Device - User Equipment.

*DoNAS. Data over Non-Access Stratum.

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

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

*HARQ. Hybrid Automatic Repeat Request.

*HSS. Home Subscriber Server. It is a database that contains users' subscription data, including data needed for mobility management.

*IP address. IPv6 or IPv4 address used.

*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.

*L2. Layer-2 in the 3GPP architectures it includes MAC, RLC and PDCP layers see Appendix A.

*LCID. Logical Channel ID. Is the logical channel instance of the corresponding MAC SDU.

*MAC. Medium Access Control protocol, part of L2.

*NAS. Non-Access Stratum.

*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-CSGN. Network Gateway - CIoT Serving Gateway Node.

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

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

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

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

*NIDD. Non-IP Data Delivery.

*PDCP. Packet Data Convergence Protocol part of L2.

*PLMN. Public Land Mobile Network. Combination of wireless communication services offered by a specific operator.

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

*RLC. Radio Link Protocol part of L2.

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

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

4. NB-IoT 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 bandwidth, acknowledgments, and layer-2 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 Network 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. The Open Mobile Alliance (OMA) [OMA0116] and the One Machine to Machine (OneM2M) [TR-0024] define the northbound APIs. [TS23222] defines architecture for the common API framework for 3GPP northbound APIs and [TS33122] defines security aspects for common API framework for 3GPP northbound APIs. In this case, the path is small for data transmission. The main functions of the NGW-SCEF are Connectivity path and Device Monitoring.

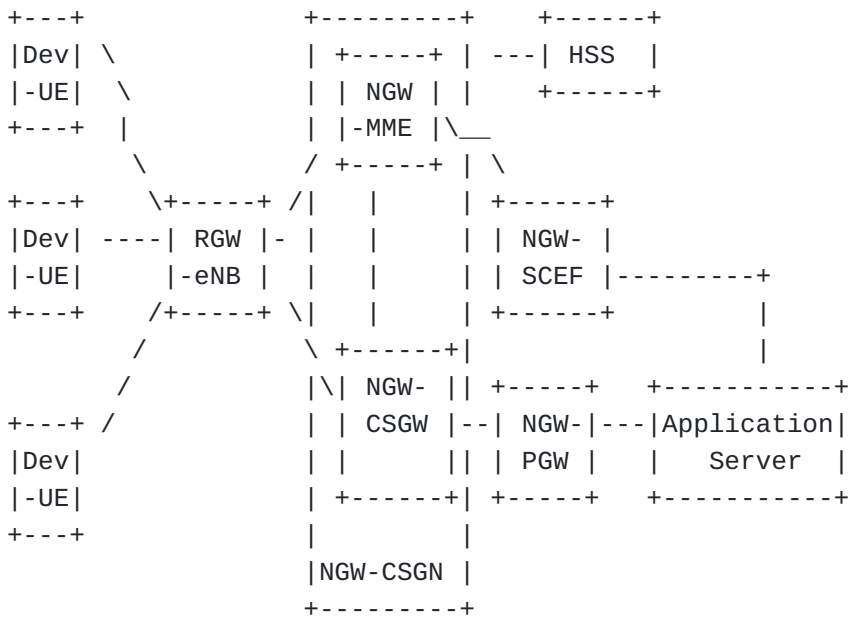


Figure 1: 3GPP network architecture

5. 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 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 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, see Section 5.2.3. However, the recommended 3GPP 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.

This document identifies the use cases of SCHC over the NB-IoT architecture.

First, the radio transmission where, see Section 5.2.1, the Dev-UE and the RGW-eNB can use the SCHC functionalities.

Second, the packets transmitted over the control path can also use SCHC when the transmission goes over the NGW-MME or NGW-SCEF. See Section 5.2.2.

These two use cases are also valid for any 3GPP architecture and not only for NB-IoT. And as the 3GPP internal network is involved, they have been put in the informational part of this section.

And third, over the SCHC over Non-IP Data Delivery (NIDD) connection or at least up to the operator network edge, see Section 5.1.1. In this case, 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. NGW-PGW or NGW-SCEF transmit the packets which are non-IP traffic, using IP tunneling or API calls. It is also possible to benefit legacy devices with SCHC by using the non-IP transmission features of the operator network.

A non-IP transmission refers to other layer-2 transport different from NB-IoT.

5.1. Normative Part.

This scenarios does not modify the 3GPP architecture or any of its components, it only use it as a layer-2 transmission.

5.1.1. SCHC over Non-IP Data Delivery (NIDD)

This section specifies the use of SCHC over Non-IP Data Delivery (NIDD) services of 3GPP. The NIDD services of 3GPP enable the transmission of SCHC packets compressed by the application layer. The packets can be delivered between the NGW-PGW and the Application Server or between the NGW-SCEF and the Application Server, using IP-tunnels or 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 over the layer-2.

5.1.1.1. SCHC Entities Placing over NIDD

In the two scenarios using NIDD compression, SCHC entities are located almost on top of the stack. The NB-IoT connectivity services implement SCHC in the Dev-UE, 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.

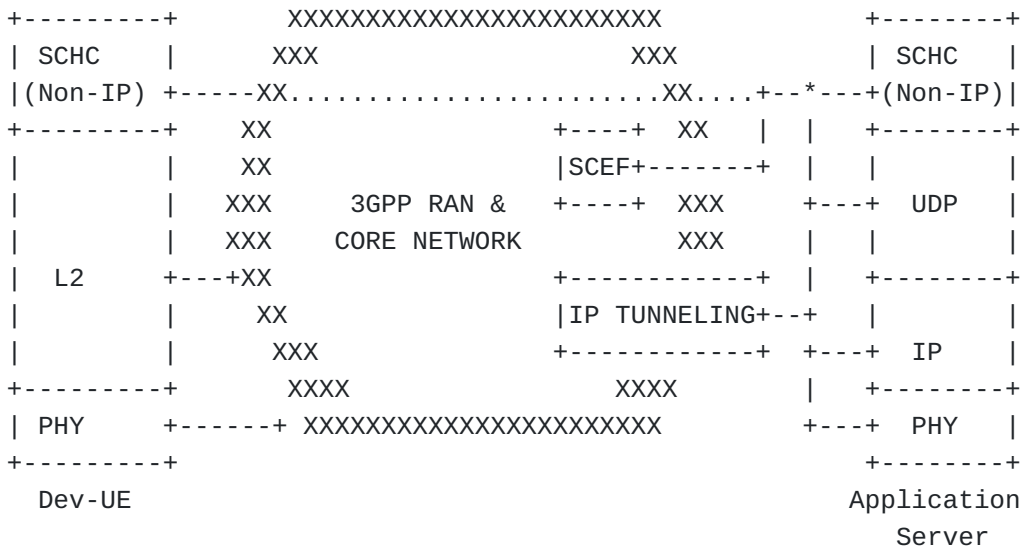


Figure 2: End-to End Compression. SCHC entities placed when using Non-IP Delivery (NIDD) 3GPP Services

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

These scenarios **MAY** use SCHC header compression capability to improve the transmission of IPv6 packets.

*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.

For devices acting as a capillary gateway, several rules match the diversity of devices and protocols used by the devices associated with the gateway. Meanwhile, simpler devices may have predetermined protocols and fixed parameters.

*Rule ID.

This scenario 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. 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 to optimize the transmission. The packets handled by 3GPP networks are byte-aligned. Thus, to use the smallest TB, the maximum SCHC header size is 12 bits. On the other hand, more complex NB-IoT devices (such as a capillary gateway) might require additional bits to handle the variety and multiple parameters of higher-layer protocols deployed. The configuration may be part of the agreed operation profile and 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 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.

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 e.g. 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 capillary 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 could be desirable to keep track of all the SCHC packets delivered. In that case, the fragmentation function could be activated for all packets transmitted by the applications. SCHC ACK-on-Error fragmentation **MAY** be activated 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 5.2.3 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 304 bits using an 8-bit 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-bit 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.

*WINDOW_SIZE of 2^N-1 is **RECOMMENDED**.

*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 use the Power Save Mode and the Idle Mode DRX, which govern how often the device wakes up, stays up, and is reachable. The use of the different modes allows the battery to last ten years. Table 10.5.163a in [TS24008] 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.

5.2. Informational Part.

These scenarios shows how 3GPP could use SCHC for their transmissions.

5.2.1. 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 3 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 A gives more details about these protocols.

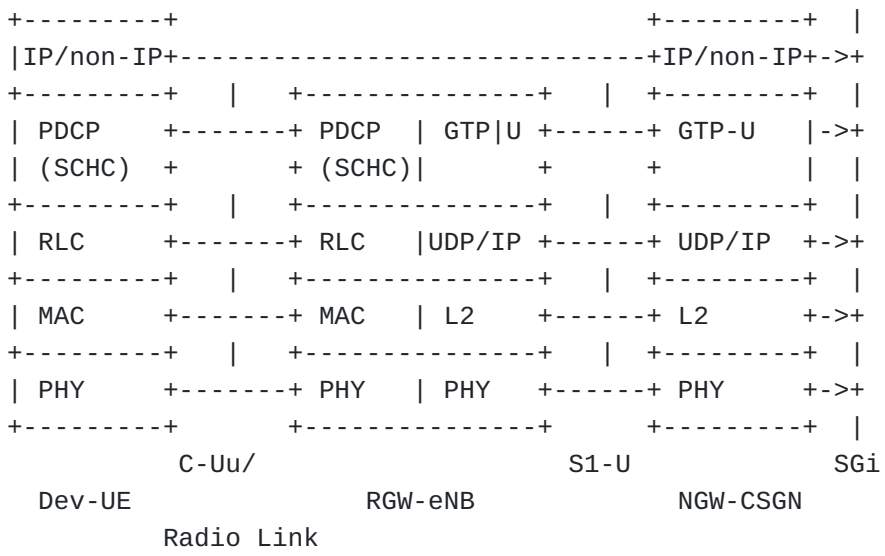


Figure 3: SCHC over the Radio link

5.2.1.1. SCHC Entities Placing over the Radio Link

The 3GPP architecture supports Robust Header Compression (ROHC) [RFC5795] in the PDCP layer. Therefore, the architecture can deploy SCHC header compression entities similarly without the need for significant changes in the 3GPP specifications.

The RLC layer has three functional modes Transparent Mode (TM), Unacknowledged Mode (UM), and Acknowledged Mode (AM). The mode of operation controls the functionalities of the RLC layer. TM only applies to signaling packets, while AM or UM carry signaling and data packets.

The RLC layer takes care of fragmentation unless for the Transparent Mode. In AM or UM modes, the SCHC fragmentation is unnecessary and **SHOULD NOT** be used. While sending IP packets, the Radio link does not commonly use the RLC Transparent Mode. However, if other

protocol overhead optimizations are targeted for NB-IoT traffic, SCHC fragmentation may be used for TM transmission mode in the future.

5.2.2. Use of SCHC over the Non-Access Stratum (NAS)

This section consists of IETF suggestions to the 3GPP. The NGW-MME conveys mainly signaling between the Dev-UE and the cellular network [TR24301]. The network transports this traffic on top of the radio link.

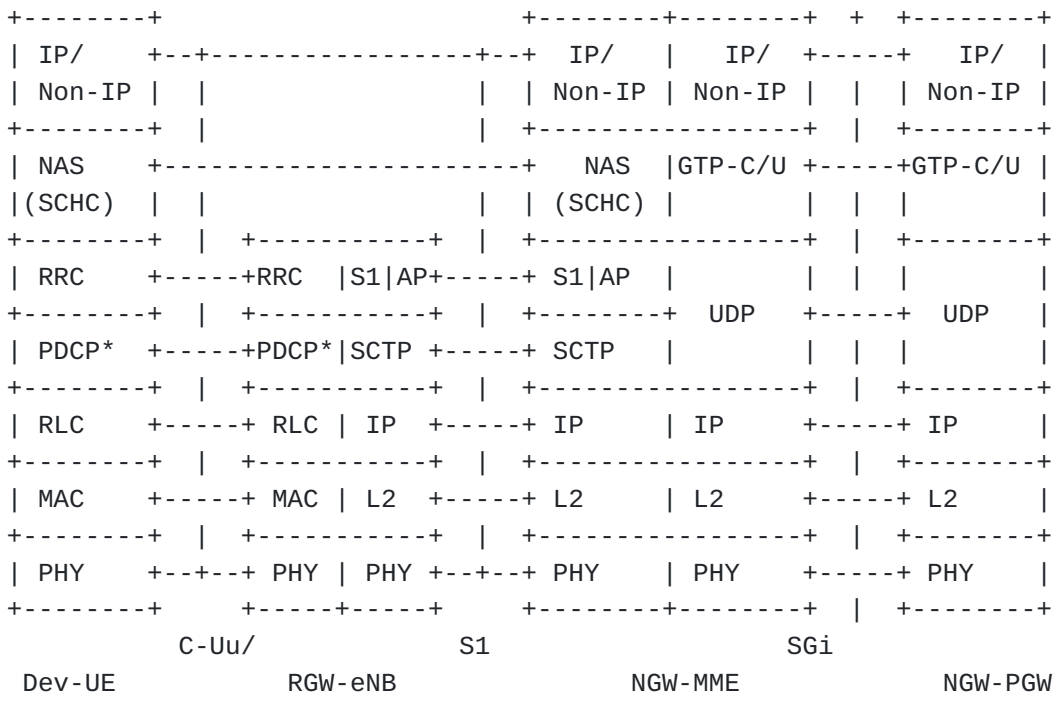
This kind of flow supports data transmissions to reduce the overhead when transmitting infrequent small quantities of data. This transmission is known as Data over Non-Access Stratum (DoNAS) or Control Plane Cellular Internet of Things (CIoT) evolved packet system (EPS) optimizations. In DoNAS, the Dev-UE 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 B gives additional details of DoNAS.

5.2.2.1. SCHC Entities Placing over DoNAS

SCHC resides in this scenario's Non-Access Stratum (NAS) protocol layer. The same principles as for the section Section 5.2.1 apply here as well. Because the NAS protocol already uses ROHC [RFC5795], it can also adapt SCHC for header compression. The main difference compared to the radio link, section Section 5.2.1, 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.



*PDCP is bypassed until AS security is activated TGPP36300.

Figure 4: SCHC entities placement in the 3GPP CIOT radio protocol architecture for DoNAS transmissions

5.2.3. Parameters for Static Context Header Compression and Fragmentation (SCHC) for the Radio link and DONAS use-cases.

If 3GPP incorporates SCHC, it is recommended that these scenarios use SCHC header compression [RFC8724] capability to optimize the data transmission.

*SCHC Context initialization.

The 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 [RFC5795] operation [TS36323].

*SCHC Rules.

The network operator in these scenarios defines the number of rules. For this, the network operator must know the IP traffic the device will carry. The operator might supply rules compatible with the device's use case. For devices acting as a capillary gateway, several rules match the diversity of devices and protocols used by

the devices associated with the gateway. Meanwhile, simpler devices may have predetermined protocols and fixed parameters. The use of IPv6 and IPv4 may force to get more 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. As for Section 5.1.1.2, these scenarios must optimize the physical layer where the smallest TB 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 capillary gateway) might require additional bits to handle the variety and multiple parameters of higher-layer protocols deployed. In that sense, the operator may want flexibility on the number and type of rules independently supported by each device; consequently, these scenarios require a configurable value. The configuration may be part of the agreed operation profile 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 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 Radio link Section 5.2.1 and DoNAS' Section 5.2.2 scenarios, the SCHC fragmentation functions are disabled. The RLC layer of NB-IoT can segment packets into 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 intrinsically.

*Fragmentation in RLC Transparent Mode.

The RLC Transparent Mode mostly applies to control signaling transmissions. When RLC operates in Transparent Mode, the MAC layer mechanisms ensure reliability and generate overhead. This additional reliability implies sending repetitions or automatic retransmissions.

The ACK-Always fragmentation mode of SCHC may reduce this overhead in future operations when data transmissions may use this mode. ACK-Always mode may 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 5.1.1.2.

6. Padding

NB-IoT and 3GPP wireless access, in general, assumes byte-aligned payload. Therefore, the layer 2 word for NB-IoT **MUST** be considered 8 bits, and the padding treatment should use this value accordingly.

7. IANA considerations

This document has no IANA actions.

8. Security considerations

This document does not add any security considerations and follows the [RFC8724] and the 3GPP access security document specified in [TS33122].

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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

[RFC8824] Minaburo, A., Toutain, L., and R. Andreasen, "Static Context Header Compression (SCHC) for the Constrained Application Protocol (CoAP)", RFC 8824, DOI 10.17487/RFC8824, June 2021, <https://www.rfc-editor.org/info/rfc8824>.

9.2. Informative References

[OMA0116] OMA, "Common definitions for RESTful Network APIs", 2018, <https://www.openmobilealliance.org/release/REST_NetAPI_Common/V1_0-20180116-A/OMA-TS-REST_NetAPI_Common-V1_0-20180116-A.pdf>.

[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>.

[TR-0024] OneM2M, "3GPP_Interworking", 2020, <https://ftp.onem2m.org/work%20programme/WI-0037/TR-0024-3GPP_Interworking-V4_3_0.DOCX>.

[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", 2019, <https://www.3gpp.org/ftp//Specs/archive/24_series/24.301/24301-f80.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>.

[TS23222] 3GPP, "Common API Framework for 3GPP Northbound APIs", 2022, <https://www.3gpp.org/ftp/Specs/archive/23_series/23.222/23222-f60.zip>.

[TS24008] 3GPP, "Mobile radio interface layer 3 specification.", 2018, <https://www.3gpp.org/ftp//Specs/archive/24_series/24.008/24008-f50.zip>.

[TS33122] 3GPP, "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs", 2018, <https://www.3gpp.org/ftp//Specs/archive/33_series/33.122/33122-f30.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>.

[TS36331] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification", 2018, <https://www.3gpp.org/ftp//Specs/archive/36_series/36.331/36331-f51.zip>.

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

Appendix A. NB-IoT User Plane protocol architecture

A.1. Packet Data Convergence Protocol (PDCP) *[TS36323]*

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 [RFC5795]

*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

A.2. Radio Link Protocol (RLC) *[TS36322]*

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 octet-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.

A.3. Medium Access Control (MAC) *[TR36321]*

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 Hybrid Automatic Repeat reQuest (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.

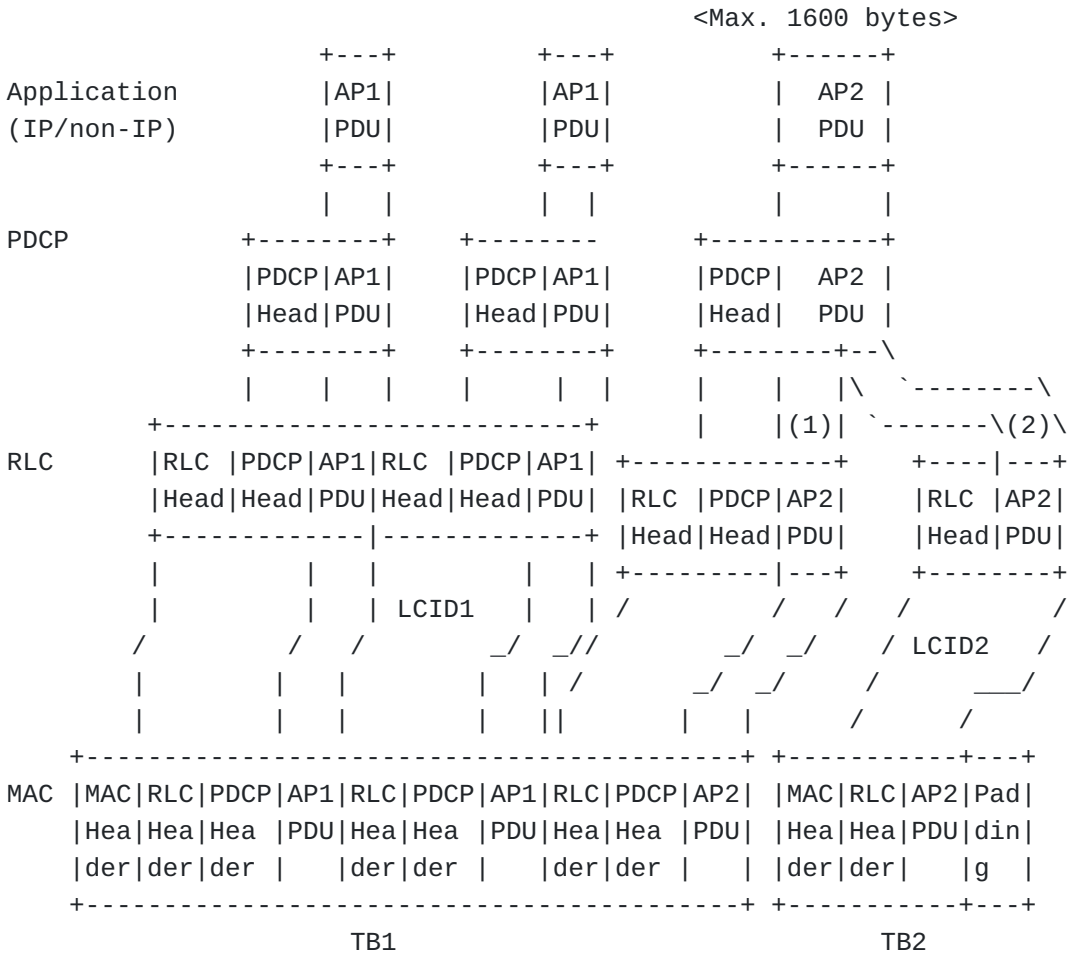


Figure 5: Example of User Plane packet encapsulation for two transport blocks

Appendix B. NB-IoT Data over NAS (DoNAS)

The Access Stratum (AS) protocol stack used by DoNAS is specific because the radio network still needs to establish the security associations and reduce the protocol overhead, so the 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 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 1600 bytes. NAS packets are encapsulated within an RRC (Radio Resource Control) [TS36331] 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.

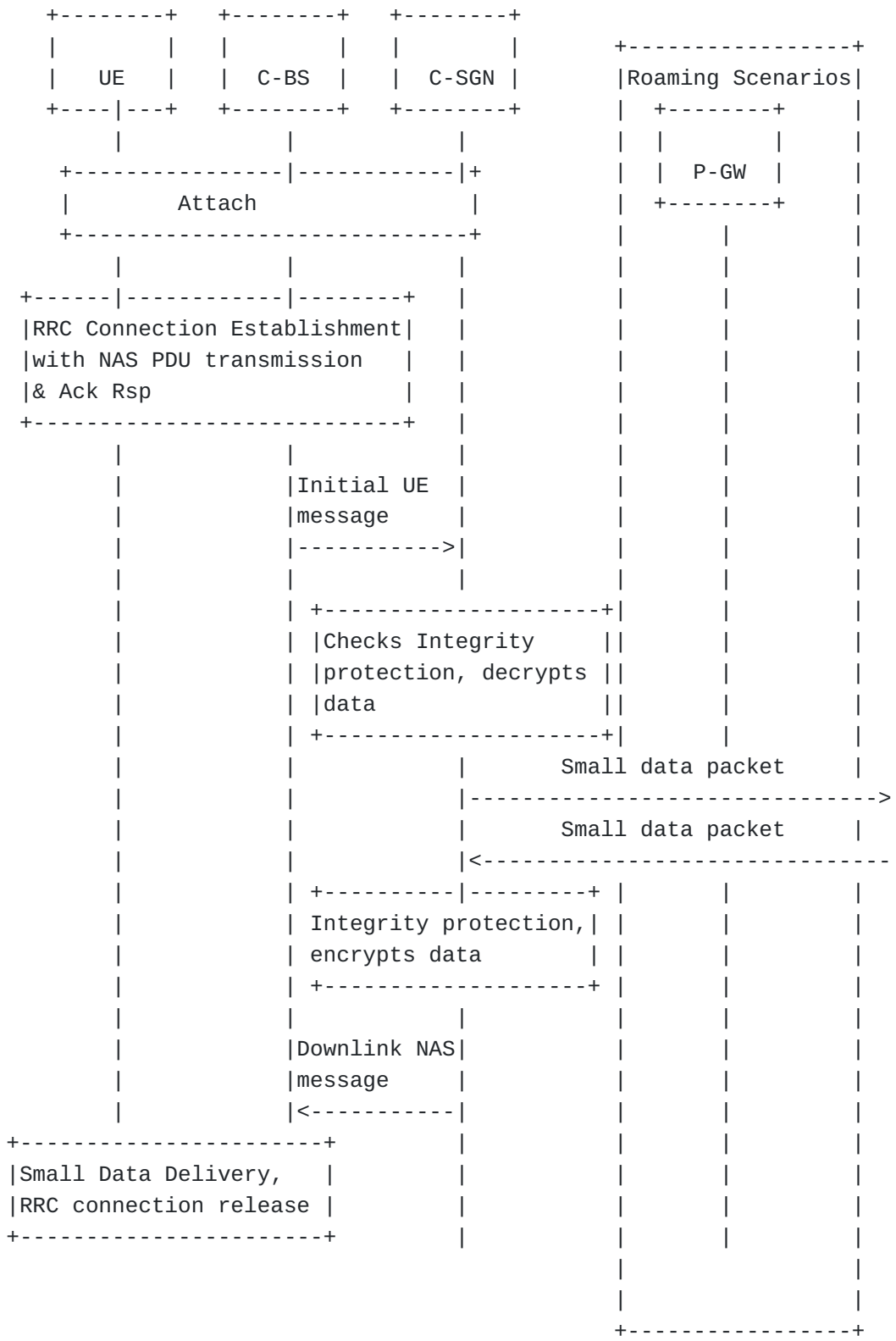


Figure 6: DoNAS transmission sequence from an Uplink initiated access

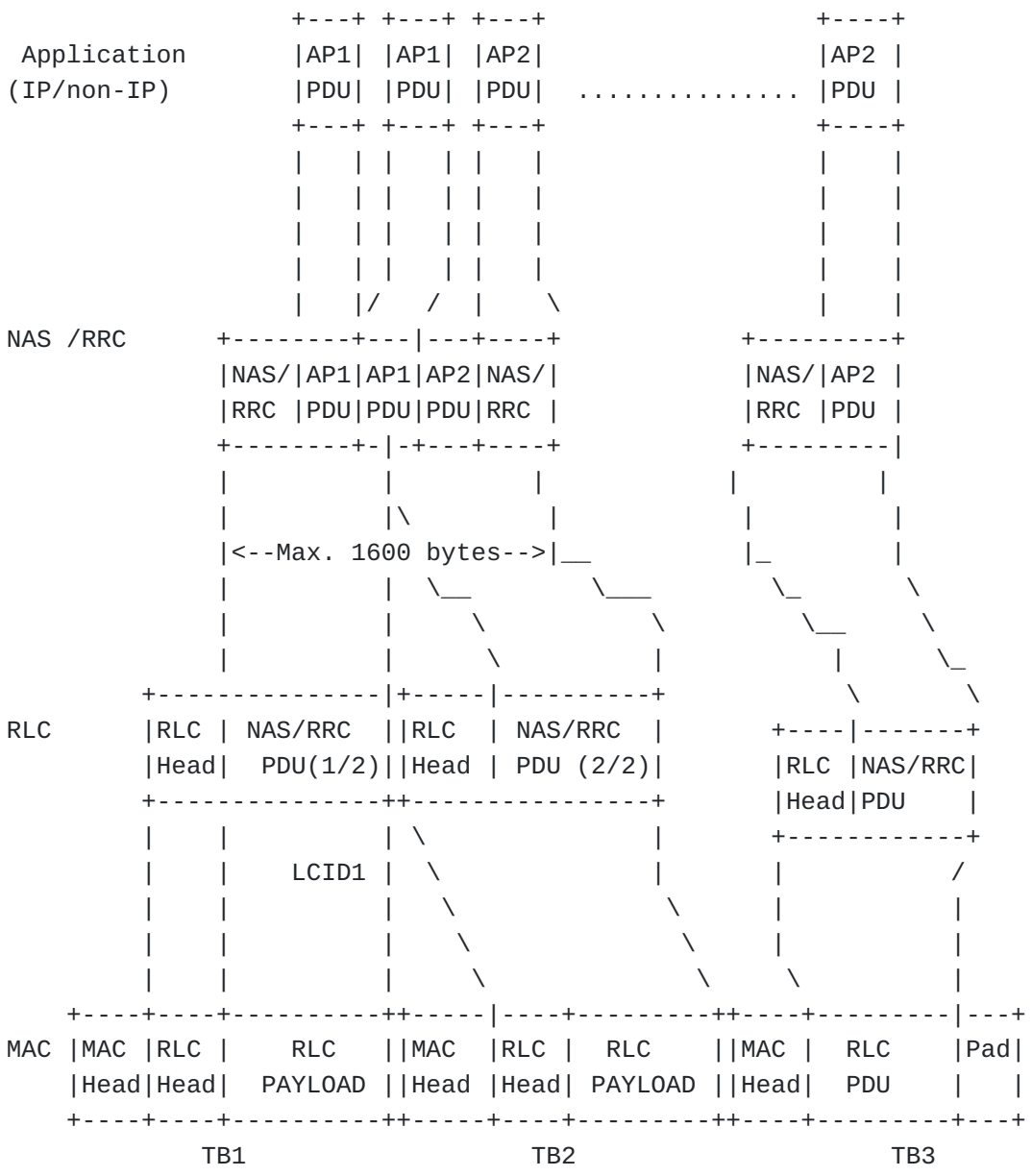


Figure 7: Example of User Plane packet encapsulation for Data over NAS

Appendix C. Acknowledgements

The authors would like to thank (in alphabetic order): Carles Gomez, Antti Ratilainen, Tuomas Tirronen, Pascal Thubert, Eric Vyncke.

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