

---

Stream: Internet Engineering Task Force (IETF)  
RFC: [9391](#)  
Category: Standards Track  
Published: April 2023  
ISSN: 2070-1721  
Authors: E. Ramos A. Minaburo  
*Ericsson Acklio*

# RFC 9391

## Static Context Header Compression over Narrowband Internet of Things

---

### Abstract

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

This document has two parts: one normative part that specifies the use of SCHC over NB-IoT and one informational part that recommends some values if 3GPP wants to use SCHC inside their architectures.

### Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc9391>.

### Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions

with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction	3
2. Conventions and Definitions	3
3. Terminology	3
4. NB-IoT Architecture	5
5. Data Transmission in the 3GPP Architecture	6
5.1. Normative Scenarios	6
5.1.1. SCHC over Non-IP Data Delivery (NIDD)	6
5.2. Informational Scenarios	9
5.2.1. Use of SCHC over the Radio Link	9
5.2.2. Use of SCHC over the Non-Access Stratum (NAS)	10
5.2.3. Parameters for Static Context Header Compression and Fragmentation (SCHC) for the Radio Link and DoNAS Use Cases	12
6. Padding	13
7. IANA Considerations	14
8. Security Considerations	14
9. References	14
9.1. Normative References	14
9.2. Informative References	14
Appendix A. NB-IoT User Plane Protocol Architecture	16
A.1. Packet Data Convergence Protocol (PDCP)	16
A.2. Radio Link Protocol (RLC)	16
A.3. Medium Access Control (MAC)	17
Appendix B. NB-IoT Data over NAS (DoNAS)	18
Acknowledgements	21
Authors' Addresses	21

## 1. Introduction

This document defines scenarios where Static Context Header Compression and fragmentation (SCHC) [RFC8724] [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 UE (Dev-UE), the radio (RGW-eNB) and network (NGW-MME) gateways, and the Application Server. This document describes the SCHC parameters supporting SCHC over the NB-IoT architecture.

This document assumes functionality for NB-IoT of 3GPP release 15 [R15-3GPP]. Otherwise, the text explicitly mentions other versions' functionality.

This document has two parts: normative end-to-end scenarios 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], [RFC8376], and [TR23720].

**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).

**Cellular IoT Evolved Packet System (CIoT EPS):** A functionality to improve the support of small data transfers.

**Device UE (Dev-UE):** As defined in [RFC8376], Section 3.

**Data over Non-Access Stratum (DoNAS):** Sending user data within signaling messages over the NAS functional layer.

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

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

Hybrid Automatic Repeat reQuest (HARQ): A combination of high-rate Forward Error Correction (FEC) and Automatic Repeat reQuest (ARQ) error control.

Home Subscriber Server (HSS): A database that contains users' subscription data, including data needed for mobility management.

IP address: IPv6 or IPv4 address used.

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

Layer 2 (L2): L2 in the 3GPP architectures includes MAC, RLC, and PDCP layers; see [Appendix A](#).

Logical Channel ID (LCID): The logical channel instance of the corresponding MAC SDU.

Medium Access Control (MAC) protocol: Part of L2.

Non-Access Stratum (NAS): Functional layer for signaling messages that establishes communication sessions and maintains the communication while the user moves.

Narrowband IoT (NB-IoT): A 3GPP Low-Power WAN (LPWAN) technology based on the LTE architecture but with additional optimization for IoT and using a Narrowband spectrum frequency.

Network Gateway - CIoT Serving Gateway Node (NGW-CSGN): As defined in [\[RFC8376\]](#), [Section 3](#).

Network Gateway - Cellular Serving Gateway (NGW-CSGW): Routes and forwards the user data packets through the access network.

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

Network Gateway - Packet Data Network Gateway (NGW-PGW): An interface between the internal and external network.

Network Gateway - Service Capability Exposure Function (NGW-SCEF): EPC node for exposure of 3GPP network service capabilities to third party applications.

Non-IP Data Delivery (NIDD): End-to-end communication between the UE and the Application Server.

Packet Data Convergence Protocol (PDCP): Part of L2.

Public Land-based Mobile Network (PLMN): A combination of wireless communication services offered by a specific operator.

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

Radio Link Protocol (RLC): Part of L2.

Radio Gateway - evolved Node B (RGW-eNB): Base Station that controls the UE.

Service Data Unit (SDU): 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 NB-IoT architecture has a complex structure. It relies on different Network Gateways (NGWs) from different providers. It can send data via different paths, each with different characteristics in terms of bandwidth, acknowledgments, and L2 reliability and segmentation.

Figure 1 shows this architecture, where the Network Gateway - Cellular IoT 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 the 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. [TS33122] defines security aspects for a 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 path connectivity and device monitoring.

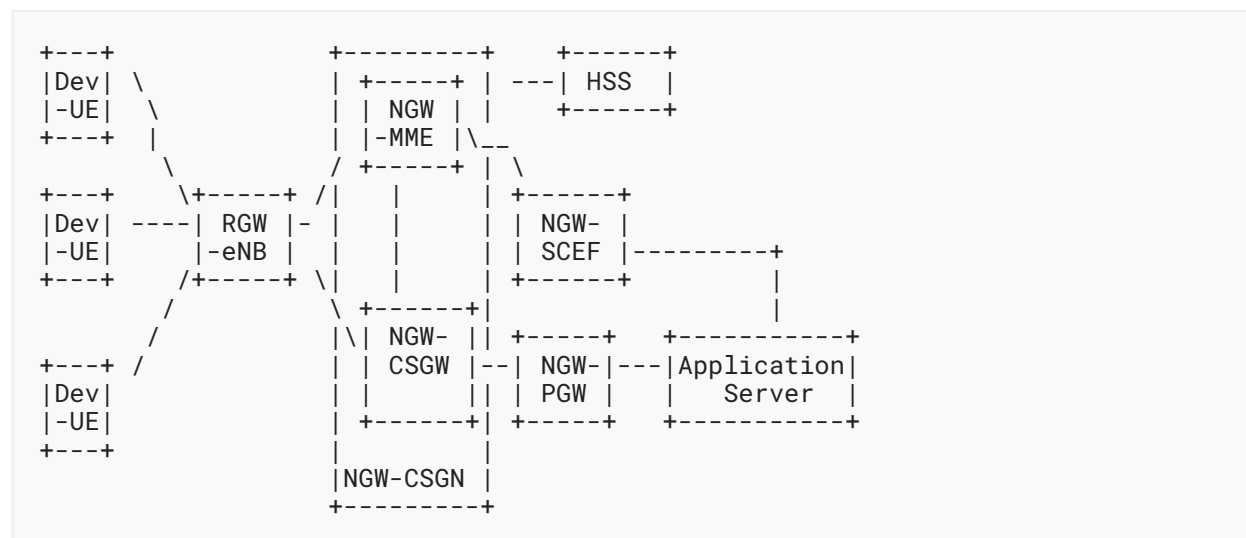


Figure 1: 3GPP Network Architecture

## 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 interfaces and functions of cellular technologies. 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.

The first use case is of the radio transmission (see [Section 5.2.1](#)) where the Dev-UE and the RGW-eNB can use the SCHC functionalities.

The second is where 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 the third covers 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 that 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 an L2 transport that is different from NB-IoT.

### 5.1. Normative Scenarios

These scenarios do not modify the 3GPP architecture or any of its components. They only use the architecture as an L2 transmission.

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

This section specifies the use of SCHC over 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 L2.

#### 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, and 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.

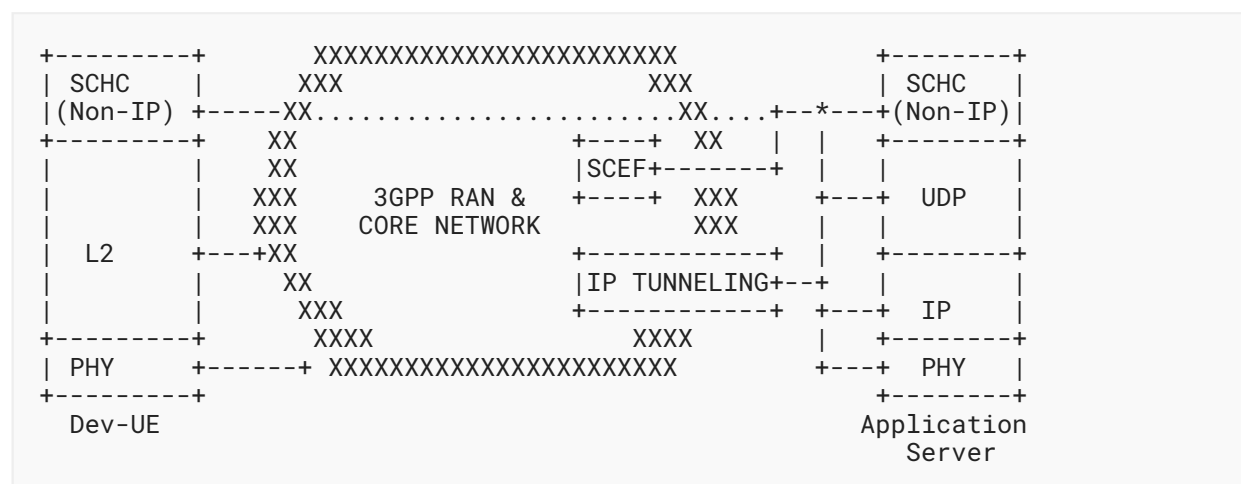


Figure 2: End-to-End Compression: SCHC Entities Placed when Using Non-IP Delivery (NIDD) 3GPP Services

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

These scenarios **MAY** use the 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 context delivery may use the same IP tunneling or NGW-SCEF services used later for the transport of SCHC packets.

- 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.

- RuleID

This scenario can dynamically set the RuleID size before the context delivery, for example, by negotiating 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 Transport Block (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, yielding up to 256 rules for use by operators. A 256-rule maximum limit seems to be quite reasonable, 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 in 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, e.g., 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 5.2.3](#) defines the RuleID size.



SCHC parametrization considers that NB-IoT 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 a multiple of 4. The Tiles **MAY** keep a fixed value of 4 or 8 bits to avoid padding, except for when the transfer block equals 16 bits as the 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 than 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**.
- Reassembly Check Sequence (RCS) will follow the default size defined in [Section 8.2.3](#) of [\[RFC8724\]](#), 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 transfers and use the Power Save Mode and the Idle Mode Discontinuous Reception (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 [\[TS24008\]](#) defines the radio timer values with units incrementing by N. The units of N can be 1 hour or 10 hours. The range used for IoT is of N to 3N, where N increments by one. The Inactivity Timer and the Retransmission Timer can be set based on these limits.

## 5.2. Informational Scenarios

These scenarios show 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 (MCSs). Transport Block (TB) transmissions happen in the Physical Layer at network-synchronized intervals called Transmission Time Interval (TTI). Each TB has a different MCS and number of bits available to transmit. The MAC layer [TR36321] defines the characteristics of the TBs. The Radio Link stack shown in Figure 3 comprises the Packet Data Convergence Protocol (PDCP) [TS36323], the Radio Link Protocol (RLC) [TS36322], the Medium Access Control protocol (MAC) [TR36321], and the Physical Layer [TS36201]. Appendix A gives more details about these protocols.

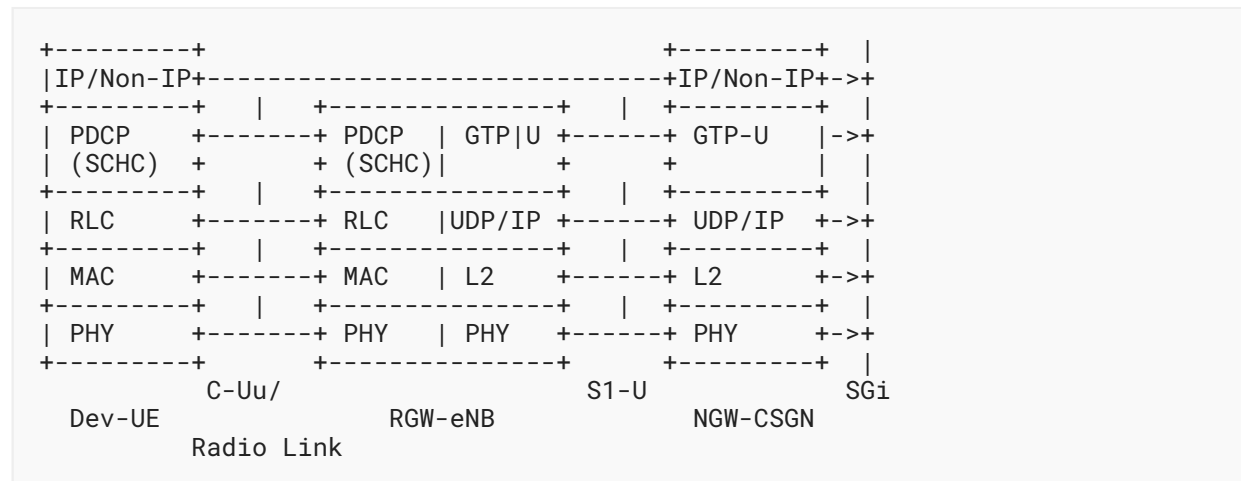


Figure 3: SCHC over the Radio Link

#### 5.2.1.1. Placing SCHC Entities 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 except for the TM. In AM or UM, the SCHC fragmentation is unnecessary and **SHOULD NOT** be used. While sending IP packets, the Radio Link does not commonly use the RLC TM. However, if other protocol overhead optimizations are targeted for NB-IoT traffic, SCHC fragmentation may be used for TM transmission 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 CIoT EPS optimizations. In DoNAS, the Dev-UE uses the pre-established security, 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 the buffered data to be transmitted, the Dev-UE might deploy the connected mode transmission instead. The connected mode would limit and control the DoNAS transmissions to predefined thresholds, and it would be a good resource optimization balance for the terminal and the network. The support for mobility of DoNAS is present but produces additional overhead. [Appendix B](#) gives additional details of DoNAS.

#### **5.2.2.1. Placing SCHC Entities over DoNAS**

SCHC resides in this scenario's Non-Access Stratum (NAS) protocol layer. The same principles as for [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 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.

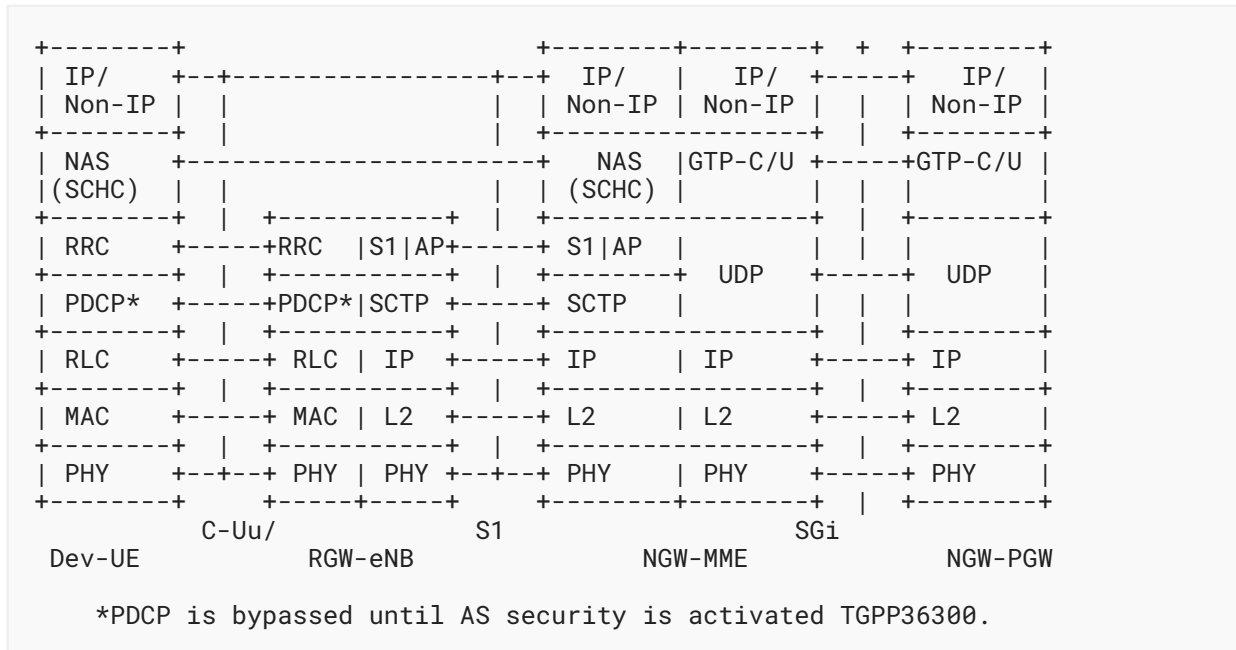


Figure 4: SCHC Entities Placement in the 3GPP CIOT Radio Protocol Architecture for DoNAS Transmissions

### 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 the SCHC header compression [RFC8724] capability to optimize the data transmission.

- SCHC Context Initialization

The Radio Resource Control (RRC) 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 been made for ROHC operation [RFC5795] [TS36323].

- SCHC Rules

The network operator defines the number of rules in these scenarios. 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 the operator to develop 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 where RLC and MAC use 4 bytes. The minimum physical TBs that can withhold this overhead value, according to the 3GPP Release 15 specification [R15-3GPP], 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, yielding up to 256 rules for use with the operators. A 256-rule maximum limit seems to be quite reasonable, 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 that is handled by the radio protocols, which corresponds to 1600 bytes for the 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 TB 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 TTI, resulting in varying physical TBs 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 TM

The RLC TM mostly applies to control signaling transmissions. When RLC operates in TM, 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. The ACK-Always mode may transmit compressed data with fewer possible transmissions by using fixed or limited TBs 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 a byte-aligned payload. Therefore, the L2 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 [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 J.C. 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] Open Mobile Alliance, "Common definitions for RESTful Network APIs", Version 1.0, January 2018, <[https://www.openmobilealliance.org/release/REST\\_NetAPI\\_Common/V1\\_0-20180116-A/OMA-TS-REST\\_NetAPI\\_Common-V1\\_0-20180116-A.pdf](https://www.openmobilealliance.org/release/REST_NetAPI_Common/V1_0-20180116-A/OMA-TS-REST_NetAPI_Common-V1_0-20180116-A.pdf)>.
- [R15-3GPP] 3GPP, "Release 15", April 2019, <<https://www.3gpp.org/specifications-technologies/releases/release-15>>.
- [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", TR-0024-V4.3.0, March 2020, <[https://ftp.onem2m.org/work%20programme/WI-0037/TR-0024-3GPP\\_Interworking-V4\\_3\\_0.DOCX](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", 3GPP TR 23.720 V13.0.0, March 2016, <[https://www.3gpp.org/ftp/Specs/archive/23\\_series/23.720/23720-d00.zip](https://www.3gpp.org/ftp/Specs/archive/23_series/23.720/23720-d00.zip)>.
- [TR24301]** 3GPP, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3", 3GPP TS 24.301 V15.8.0, December 2019, <[https://www.3gpp.org/ftp/Specs/archive/24\\_series/24.301/24301-f80.zip](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", 3GPP TS 36.321 V13.2.0, June 2016, <[https://www.3gpp.org/ftp/Specs/archive/36\\_series/36.321/36321-d20.zip](https://www.3gpp.org/ftp/Specs/archive/36_series/36.321/36321-d20.zip)>.
- [TS23222]** 3GPP, "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2", 3GPP TS 23.222 V15.6.0, September 2022, <[https://www.3gpp.org/ftp/Specs/archive/23\\_series/23.222/23222-f60.zip](https://www.3gpp.org/ftp/Specs/archive/23_series/23.222/23222-f60.zip)>.
- [TS24008]** 3GPP, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3", 3GPP TS 24.008 V15.5.0, December 2018, <[https://www.3gpp.org/ftp/Specs/archive/24\\_series/24.008/24008-f50.zip](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", 3GPP TS 33.122 V15.3.0, March 2019, <[https://www.3gpp.org/ftp/Specs/archive/33\\_series/33.122/33122-f30.zip](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", 3GPP TS 36.201 V15.1.0, June 2018, <[https://www.3gpp.org/ftp/Specs/archive/36\\_series/36.201/36201-f10.zip](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", 3GPP TS 36.322 V15.0.1, April 2018, <[https://www.3gpp.org/ftp/Specs/archive/36\\_series/36.322/36322-f01.zip](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", 3GPP TS 36.323 V13.2.0, June 2016, <[https://www.3gpp.org/ftp/Specs/archive/36\\_series/36.323/36323-d20.zip](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", 3GPP TS 36.331 V15.5.1, April 2019, <[https://www.3gpp.org/ftp/Specs/archive/36\\_series/36.331/36331-f51.zip](https://www.3gpp.org/ftp/Specs/archive/36_series/36.331/36331-f51.zip)>.
-



## Appendix A. NB-IoT User Plane Protocol Architecture

### A.1. Packet Data Convergence Protocol (PDCP)

Each of the Radio Bearers (RBs) is associated with one PDCP entity [TS36323]. Moreover, a PDCP entity is associated with one or two RLC entities, depending on the unidirectional or bidirectional 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 is in use for User Plane only)
- Ciphering and deciphering
- Timer-based SDU discard in uplink

### A.2. Radio Link Protocol (RLC)

RLC [TS36322] is an L2 protocol that operates between the User Equipment (UE) and the base station (eNB). It supports the packet delivery from higher layers to MAC, creating packets transmitted over the air, optimizing the TB 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 bidirectional 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 (e.g., status reports) between entities. RLC can be configured for a 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 with 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, upon reception, a TM RLC receiver would not process the packets and only deliver them to higher layers.

- 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 lower-layer retransmissions, there is no support for re-segmentation in case the radio conditions change and trigger the selection of a smaller TB. Additionally, it provides PDU duplication detection and discards, out-of-sequence reordering, 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 Reports, and to 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)

MAC [TR36321] provides a mapping between the higher layers abstraction called Logical Channels (which are comprised by the previously described protocols) and the Physical Layer channels (transport channels). Additionally, MAC may multiplex packets from different Logical Channels and prioritize which ones to fit into one TB 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 reported from the terminal to the network. MAC also adds the necessary padding and piggyback control elements, when possible, as well as the higher layers data.

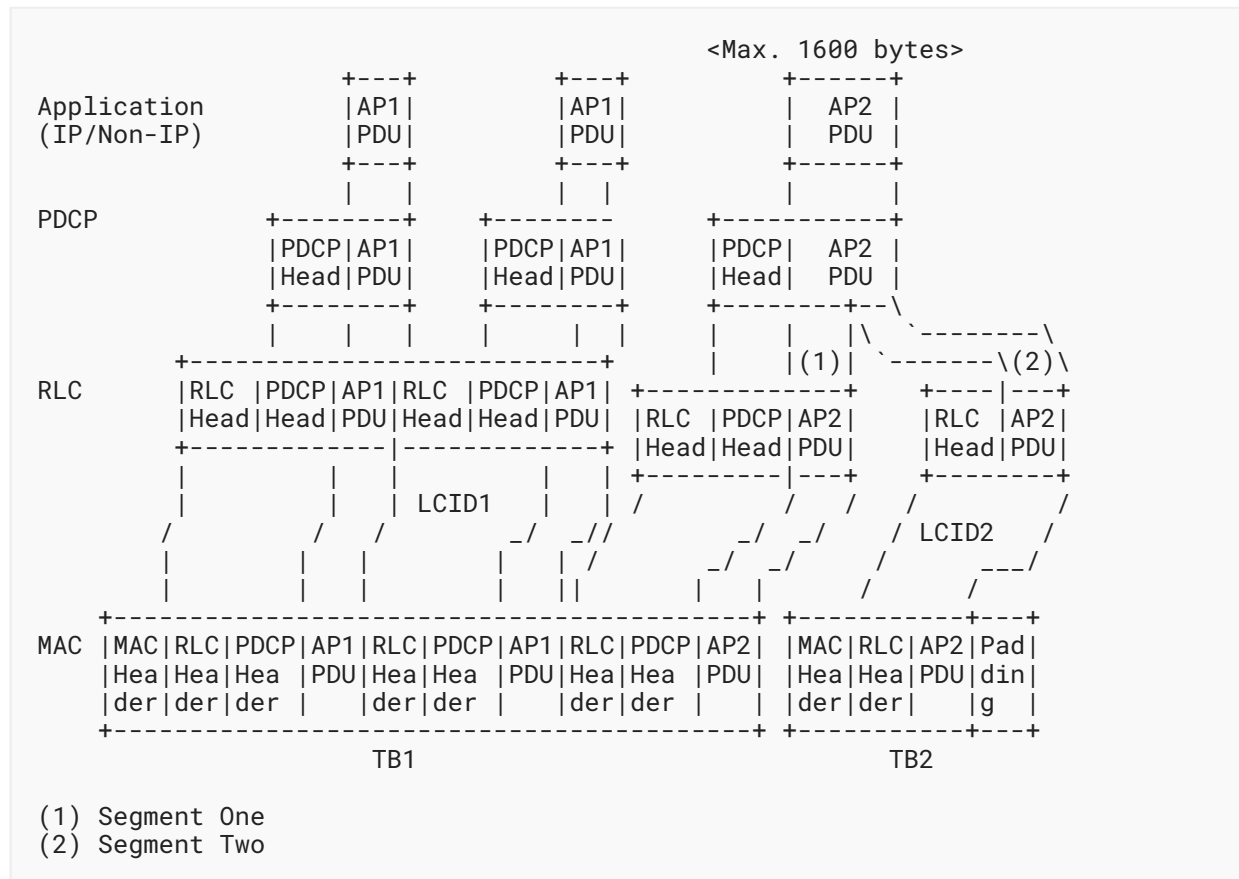


Figure 5: Example of User Plane Packet Encapsulation for Two Transport Blocks

## 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 that the PDCP is bypassed until the AS security is activated. By default, RLC uses the AM. However, depending on the network's features and the terminal, RLC may change to other modes by the network operator. For example, the TM does not add any header nor process the payload to reduce the overhead, but the MTU would be limited by the TB used to transmit the data, which is a couple of thousand bits maximum. If UM (only terminals compatible with 3GPP Release 15 [R15-3GPP]) 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 the overhead would have the same support for segmentation up to 1600 bytes. NAS packets are encapsulated within an RRC [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 is receiving an acknowledgment or short feedback from the network. Depending on the size of buffered data to be transmitted, 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.

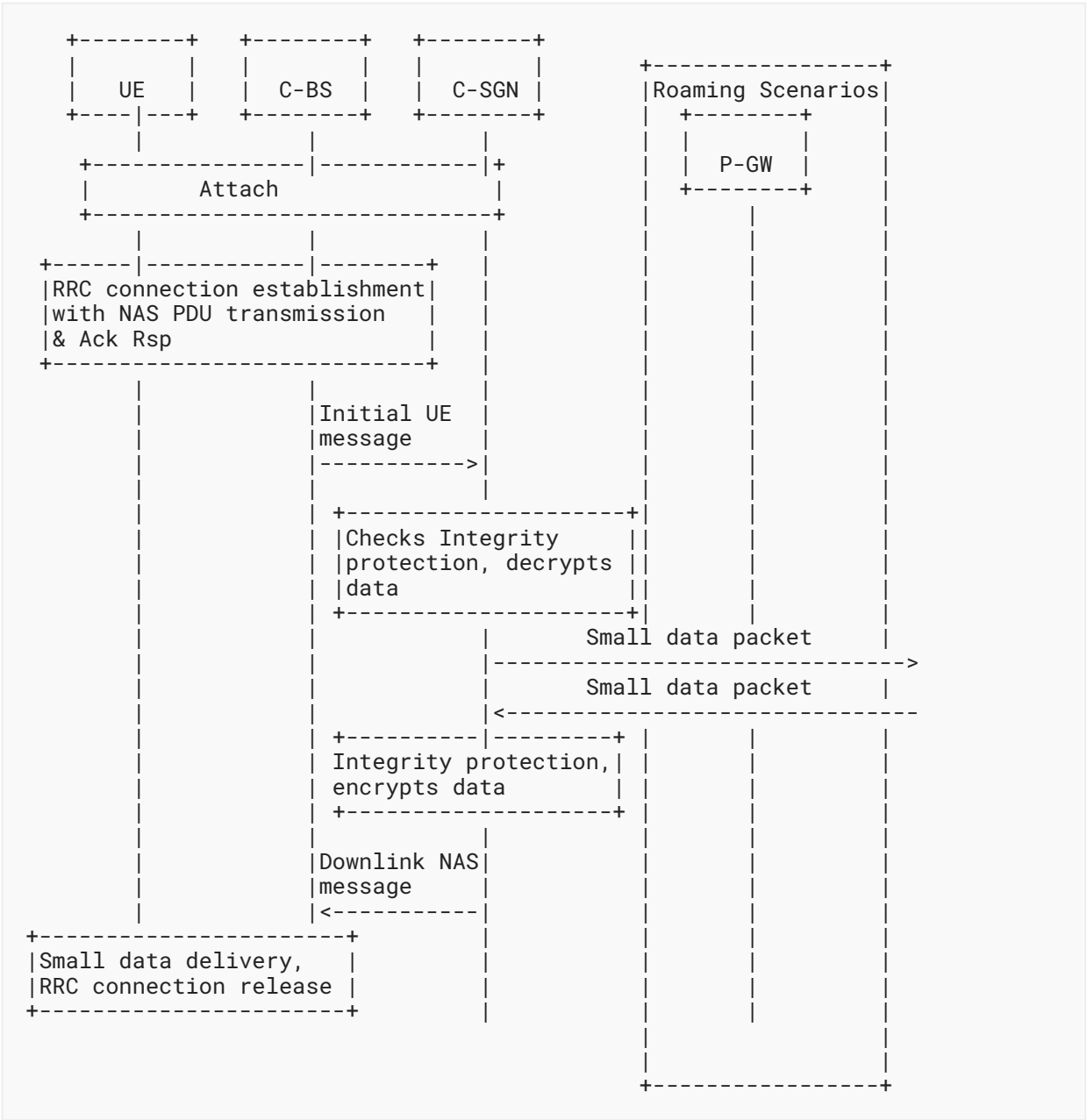


Figure 6: DoNAS Transmission Sequence from an Uplink Initiated Access

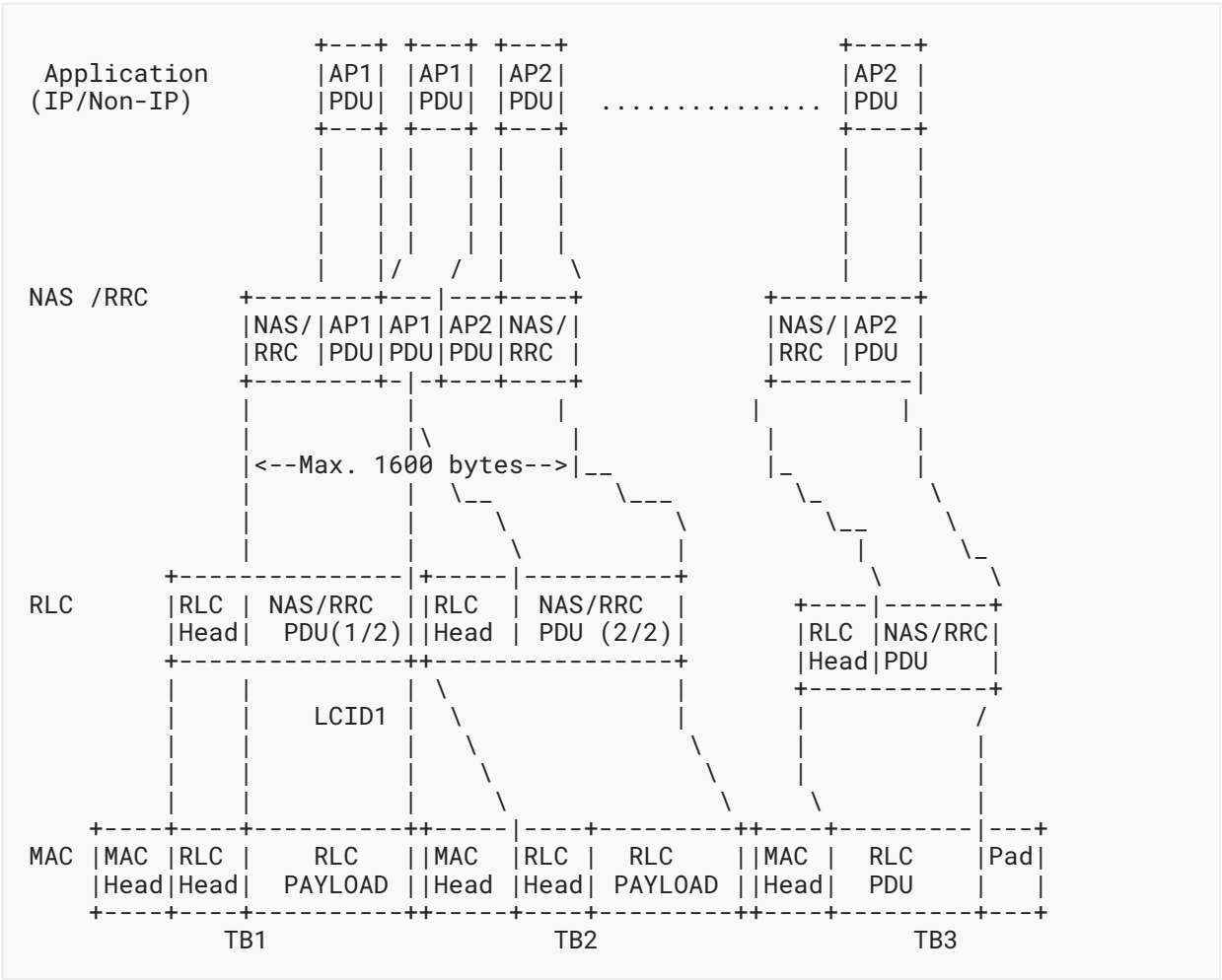


Figure 7: Example of User Plane Packet Encapsulation for Data over NAS

Acknowledgements

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

Authors' Addresses

**Edgar Ramos**  
Ericsson  
Hirsalantie 11  
FI-02420 Jorvas, Kirkkonummi  
Finland  
Email: [edgar.ramos@ericsson.com](mailto:edgar.ramos@ericsson.com)

**Ana Minaburo**

Acklio

1137A Avenue des Champs Blancs

35510 Cesson-Sevigne Cedex

France

Email: [ana@ackl.io](mailto:ana@ackl.io)