

lpwan Working Group
Internet-Draft
Intended status: Informational
Expires: 26 August 2022

E. Ramos
Ericsson
A. Minaburo
Acklio
22 February 2022

SCHC over NB-IoT
draft-ietf-lpwan-schc-over-nbiot-07

Abstract

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

This document describes the use of SCHC over the NB-IoT wireless access and provides elements for 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 26 August 2022.

Copyright Notice

Copyright (c) 2022 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

Internet-Draft

SCHC NB-IoT

February 2022

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.	Terminology	3
3.	Architecture	4
4.	Data Transmission	5
5.	IP based Data Transmission	6
5.1.	SCHC over the Radio link	6
5.1.1.	SCHC Entities Placing	6
5.2.	SCHC over No-Access Stratum (NAS)	7
5.2.1.	SCHC Entities Placing	8
5.3.	Parameters for Static Context Header Compression (SCHC)	8
5.3.1.	SCHC Context initialization	9
5.3.2.	SCHC Rules	9
5.3.3.	Rule ID	9
5.3.4.	SCHC MAX_PACKET_SIZE	10
5.3.5.	Fragmentation	10
6.	End-to-End Compression	10
6.1.	SCHC Entities Placing	11
6.2.	Parameters for Static Context Header Compression	11
6.2.1.	SCHC Context initialization	11
6.2.2.	SCHC Rules	12
6.2.3.	Rule ID	12
6.2.4.	SCHC MAX_PACKET_SIZE	12
6.3.	Fragmentation	12
6.3.1.	Fragmentation modes	12
6.3.2.	Fragmentation Parameters	13
7.	Padding	13
8.	Security considerations	13
9.	3GPP References	13
10.	Appendix	14
10.1.	NB-IoT User Plane protocol architecture	14
10.1.1.	Packet Data Convergence Protocol (PDCP)	14
10.1.2.	Radio Link Protocol (RLC)	15
10.1.3.	Medium Access Control (MAC)	16
10.2.	NB-IoT Data over NAS (DoNAS)	17
11.	Normative References	19
	Authors' Addresses	20

Internet-Draft

SCHC NB-IoT

February 2022

[1.](#) Introduction

The Static Context Header Compression (SCHC) [[RFC8724](#)] defines a header compression scheme, and fragmentation functionality suitable for the Low Power Wide Area Networks (LPWAN) networks defined in [[RFC8376](#)].

In an NB-IoT network, header compression efficiently brings Internet connectivity to the node. This document describes the SCHC parameters used to perform the static context header compression into the NB-IoT wireless access. This document assumes functionality for NB-IoT of 3GPP release 15. Otherwise, the text explicitly mentions other versions' functionality.

[2.](#) Terminology

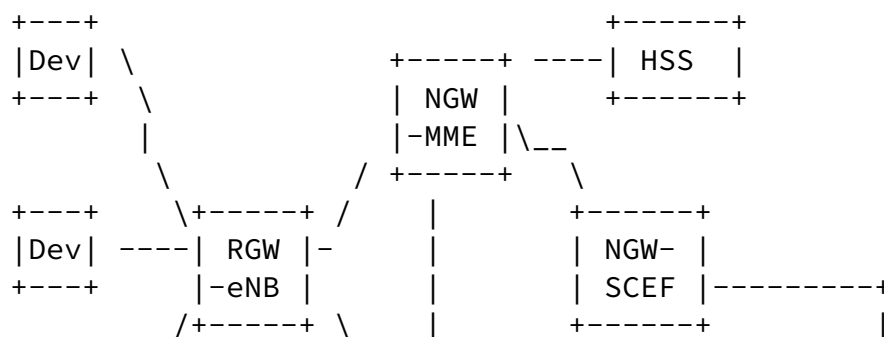
This document will follow the terms defined in [[RFC8724](#)], in [[RFC8376](#)], and the TGPP23720.

- * CIoT. Cellular IoT
- * NGW-C-SGN. Network Gateway - CIoT Serving Gateway Node
- * Dev-UE. Device - User Equipment
- * RGW-eNB. Radio Gateway - Node B. Base Station that controls the UE
- * EPC. Evolved Packet Connectivity. Core network of 3GPP LTE systems.
- * EUTRAN. Evolved Universal Terrestrial Radio Access Network. Radio network from LTE based systems.
- * NGW-MME. Network Gateway - 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.
- * NGW-SGW. Network Gateway - 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

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

[3. Architecture](#)



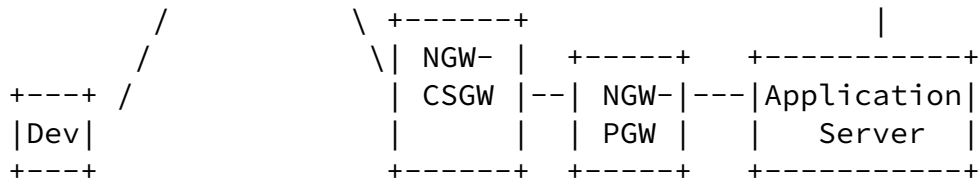


Figure 1: 3GPP network architecture

The Narrow Band Internet of Things (NB-IoT) architecture has a more complex structure. It relies on different NGWs from different providers and can send data by different paths, each path with different characteristics such as bandwidths, acknowledgments, and layer two reliability and segmentation.

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

Another node introduced in the NBIoT architecture is the Network Gateway Service Capability Exposure Function (NGW-SCEF), which securely exposes service and network capabilities to entities external to the network operator. OMA and OneM2M define the northbound APIS [TGPP33203]. In this case, the path is small for data transmission. The main functions of the NGW-SCEF are:

- * Connectivity path
- * Device Monitoring

4. Data Transmission

NB-IoT networks deal with end-to-end user data and in-band signaling

between the nodes and functions to configure, control, and monitor the system functions and behaviors. The signaling data uses a different path with specific protocols, handling processes, and entities but can transport end-to-end user data for IoT services. In contrast, the end-to-end application only transports end-to-end data.

The maximum recommended MTU size is 1358 Bytes. The radio network protocols limit the packet sizes over the air, including radio protocol overhead to 1600 Bytes. However, the 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, RGW-eNB, and NGW-CSGN needs to be specified in the NB-IoT standard, which implies that standard specifying SCHC support would not be backward compatible. A terminal or a network supporting a version of the standard without SCHC or without capability implementation (in case of not being standardized as mandatory capability) cannot 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 can be used over the radio transmission only, between

the Dev and the RGW-eNB. Alternatively, the packets transmitted over the end-to-end link can use SCHC. Else, when the transmissions over the NGW-MME or NGW-SCEF, the NGW-CSGN uses SCHC entity. 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. SCHC functionalities are available in the application layer of the Dev and the Application Servers or a broker function at the edge of the operator network. The radio network transmits the packets as non-IP traffic using IP tunneling or SCEF services. Since this option does not necessarily require 3GPP standardization, it is possible to also benefit legacy devices with SCHC by using the non-IP transmission features of the operator network.

[5.](#) IP based Data Transmission

[5.1.](#) SCHC over the Radio link

Deploying SCHC only over the radio link would require placing it as part of the protocol stack for data transfer between the Dev 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 Modulation and Coding Schemes (MCS) selected. A 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 [TGPP36321] defines the Transport Blocks characteristics. The Radio link Figure 2 stack comprises the Packet Data Convergence Protocol (PDCP) [TGPP36323], Radio Link Protocol (RLC) [TGPP36322], Medium Access Control protocol (MAC) [TGPP36321], and the Physical Layer [TGPP36201]. The Appendix gives more details of these protocols.

[5.1.1.](#) SCHC Entities Placing

The current architecture provides support for header compression in PDCP with RoHC [[RFC5795](#)]. Therefore SCHC entities can be deployed similarly without the need for significant changes in the 3GPP specifications.

In this scenario, RLC takes care of fragmentation unless for the transparent mode. When packets exceed the transport block size at the time of transmission, SCHC fragmentation is unnecessary and should not be used to avoid the additional protocol overhead. It is not common to configure RLC in Transparent Mode for IP-based data. However, given the case in the future, SCHC fragmentation may be used. In that case, a SCHC tile would match the minimum transport block size minus the PDCP and MAC headers.

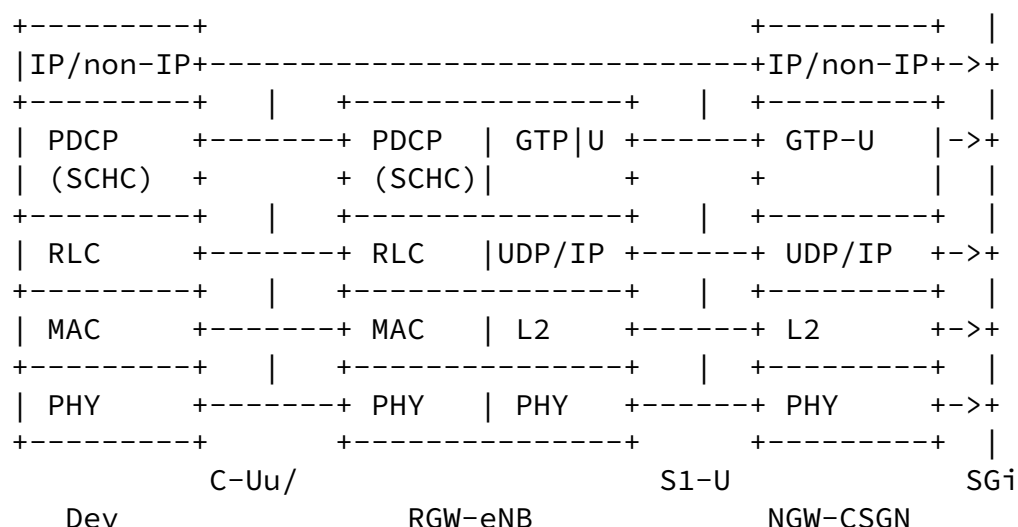


Figure 2: SCHC over the Radio link

5.2. SCHC over No-Access Stratum (NAS)

The NGW-MME conveys mainly control signaling between the Dev and the cellular network [TGPP24301]. The network transports this traffic on top of the radio link.

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

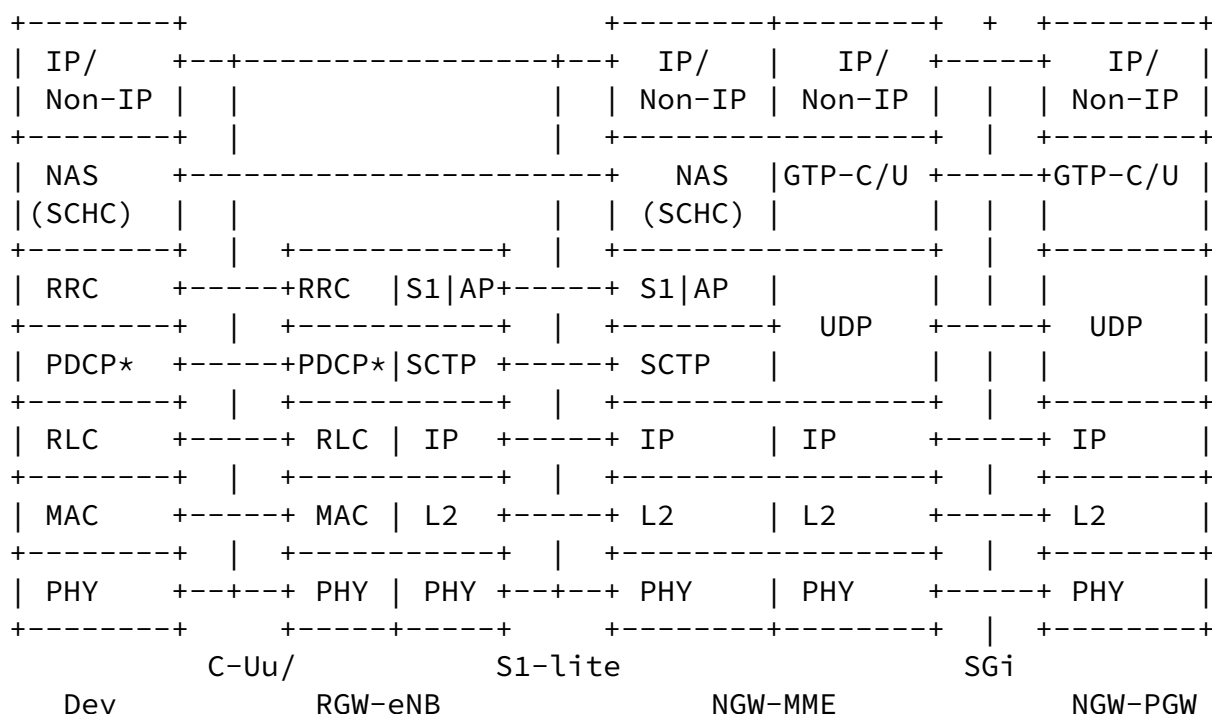
The NGW-MME performs the data encryption from the network side in a DoNAS PDU. Depending on the data type signaled indication (IP or non-IP data), the network allocates an IP address or establishes a direct forwarding path. DoNAS is regulated under rate control upon previous agreement, meaning that a 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 might deploy the connected mode transmissions instead, limiting and controlling the DoNAS transmissions to predefined thresholds and a good resource optimization balance for the terminal and the network. The support for mobility of DoNAS is present but produces additional overhead. The Appendix gives additional details of DoNAS.

5.2.1. SCHC Entities Placing

SCHC may reside in the Non-Access Stratum (NAS) protocol layer in this scenario. The same principles as for Radio link transmissions apply here as well. The main difference is the physical placing of the SCHC entities on the network side as the NGW-MME resides in the core network and is the terminating node for NAS instead of the eNB.



*PDCP is bypassed until AS security is activated TGP36300.

Figure 3

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 parameters of the Radio link. It will configure SCHC and the static context distribution as it has made for RoHC operation [TGPP36323].

[5.3.2.](#) SCHC Rules

The network operator in these scenarios defines the number of rules in a context. The operator must be aware of the type of IP traffic that the device will carry out. Implying that the operator might use provision sets of rules compatible with the use case of the device. For devices acting as gateways of other devices, several rules may match the diversity of devices and protocols used by the devices associated with the gateway. Meanwhile, simpler devices (for example, an electricity meter) may have a predetermined set of fixed protocols and parameters. Additionally, the deployment of IPv4 addresses and IPv6 may force different rules to deal with each case.

[5.3.3.](#) Rule ID

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

consider the byte-alignment of the expected Compression Residue. In the minimum TB size case, 2 bits of Rule Id leave only 6 bits

available for Compression Residue.

[5.3.4.](#) 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 that correspond to 1600 bytes for 3GPP Release 15.

[5.3.5.](#) Fragmentation

For these scenarios, the SCHC fragmentation functions are disabled. The RLC layer of NB-IoT can segment packets in suitable units that fit the selected transport blocks for transmissions of the physical layer. The blocks 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 than allowing the Radio link protocols to take care of the fragmentation natively.

[5.3.5.1.](#) Fragmentation in Transparent Mode

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

SCHC may reduce radio network protocols overhead in future operations, support reliable transmissions, and transmit small data with fewer possible transmissions by using fixed or limited transport blocks compatible with the tiling SCHC fragmentation handling.

6. End-to-End Compression

The Non-IP Data Delivery (NIDD) services of 3GPP enable the transmission of SCHC packets compressed by the application layer. The packets can be delivered using IP-tunnels to the 3GPP network or NGW-SCEF functions (i.e., API calls). In both cases, as compression occurs before transmission, the network will not understand the packet, and the network does not have context information of this

compression. Therefore the network will treat the packet as Non-IP traffic and deliver it to the Dev without any other stack element, directly under the L2.

6.1. SCHC Entities Placing

In the two scenarios using End-to-End compression, SCHC entities are located almost on top of the stack. In the Dev, an application using the NB-IoT connectivity services may implement SCHC and 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.

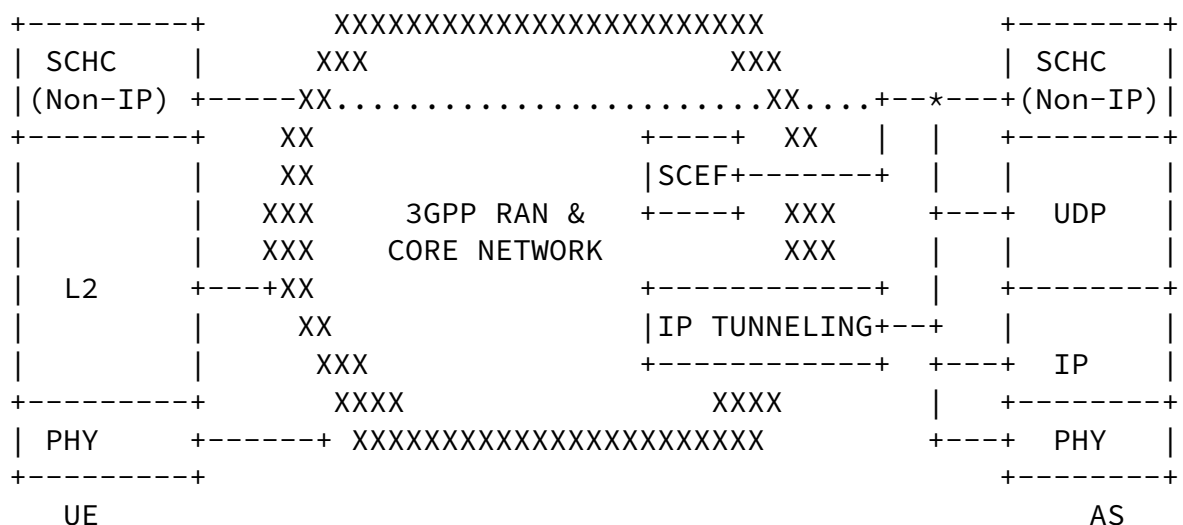


Figure 4: SCHC entities placed when using Non-IP Delivery (NIDD)
3GPP Sevicees

[6.2.](#) Parameters for Static Context Header Compression

[6.2.1.](#) 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.

[6.2.2.](#) SCHC Rules

Even when the transmission content is not visible for the 3GPP network, the same limitations as 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

Similar to the case of IP transmissions, the Rule ID size can be dynamically set before the context delivery. For example, negotiated between the applications when choosing a profile according to the type of traffic and application deployed. The same considerations related to the transport block size and performance mentioned for the IP type of traffic must be followed 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), not only the radio as the IP transmissions case.

[6.3.](#) Fragmentation

In principle, packets larger than 1358 bytes need the 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.

6.3.1. Fragmentation modes

A global service assigns a QoS to the packets depending on the billing. Packets with very low QoS may get lost before they arrive in the 3GPP radio network transmission, for example, in between the links of a capillarity gateway or due to buffer overflow handling in a backhaul connection. The use of SCHC fragmentation with the ACK-on-Error mode is recommended to secure additional reliability on the packets transmitted with a small trade-off on additional transmissions to signal the end-to-end arrival of the packets if no transport protocol takes care of retransmission. Also, the ACK-on-Error mode is even desirable to keep track of all the SCHC packets delivered. In that case, the fragmentation function could be active for all packets transmitted by the applications. SCHC ACK-on-Error fragmentation may be active for the transmission of non-IP packets on the NGW-MME. If these packets are considering to use SCHC with the

RuleID for non-compressing packets as {[RFC8724](#)} allows it.

6.3.2. Fragmentation Parameters

SCHC profile with the fragmentation mode will have specific Rules. The Rule ID will identify the fragmentation mode used, and it is defined in section [Section 5.3.3](#).

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 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 of 2 bits. For the other parameters, the transfer block size has a wide range that needs two configurations.

- * For Transfer Blocks smaller than 300bits: 8 bits-Header_size configuration, with the size of the header fields as follows: Rule

ID from 1 - 3 bits, DTag 1 bit, FCN 3 bits, W 1 bits.

- * For Transfer Blocks bigger than 300 bits: 16 bits-Header_size configuration, with the size of the header fields as follows:
Rules ID from 1 to 8 or 10 bits, DTag 1 or 2 bits, FCN 3 bits, W 2 or 3 bits.

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

[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 padding treatment should use this value accordingly.

[8.](#) Security considerations

This document does not add any security considerations and follows the 3GPP access security document 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
- * TGPP24088 3GPP, "TS 24.088 v12.9.0 - Mobile radio interface Layer 3 specification;Core network protocols; Stage 3", 2015.

[10.](#) Appendix

[10.1.](#) NB-IoT User Plane protocol architecture

[10.1.1.](#) Packet Data Convergence Protocol (PDCP)

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

- * Header compression and decompression using ROHC (Robust Header Compression)
- * Transfer of user and control data to higher and lower layers

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

- * Ciphering and deciphering
- * Timer-based SDU discard in uplink

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 transmitted over the air, optimizing the Transport Block utilization. RLC flow of data packets is unidirectional, and it is composed of a transmitter located in the transmission device and a receiver located in the destination device. Therefore to configure bi-directional flows, two sets of entities, one in each direction (downlink and uplink), must be configured and effectively peered to each other. The peering allows the transmission of control packets (ex., status reports) between entities. RLC can be configured for data transfer in one of the following modes:

- * Transparent Mode (TM). RLC does not segment or concatenate SDUs from higher layers in this mode and does not include any header to the payload. RLC receives SDUs from upper layers when acting as a transmitter and transmits directly to its flow RLC receiver via lower layers. Similarly, a TM RLC receiver would only deliver without processing the packets to higher layers upon reception.
- * Unacknowledged Mode (UM). This mode provides support for segmentation and concatenation of payload. The RLC packet's size depends on the indication given at a particular transmission opportunity by the lower layer (MAC) and is octets aligned. The packet delivery to the receiver does not include reliability support, and the loss of a segment from a packet means a complete packet loss. Also, in the case of lower layer retransmissions, there is no support for re-segmentation in case of change of the radio conditions triggering the selection of a smaller transport block. Additionally, it provides PDU duplication detection and discards, reordering of out-of-sequence, and loss detection.
- * Acknowledged Mode (AM). In addition to the same functions supported by UM, this mode also adds a moving windows-based reliability service on top of the lower layer services. It also supports re-segmentation, and it requires bidirectional communication to exchange acknowledgment reports called RLC Status Report and trigger retransmissions. This model also supports

protocol error detection. The mode used depends on the operator configuration for the type of data to be transmitted. For example, data transmissions supporting mobility or requiring high reliability would be most likely configured using AM. Meanwhile, streaming and real-time data would be mapped to a UM configuration.

[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 data transmission efficiency. MAC also provides error correction and reliability support through HARQ, transport format selection, and scheduling information reporting from the terminal to the network. MAC also adds the necessary padding and piggyback control elements when possible and the higher layers data.

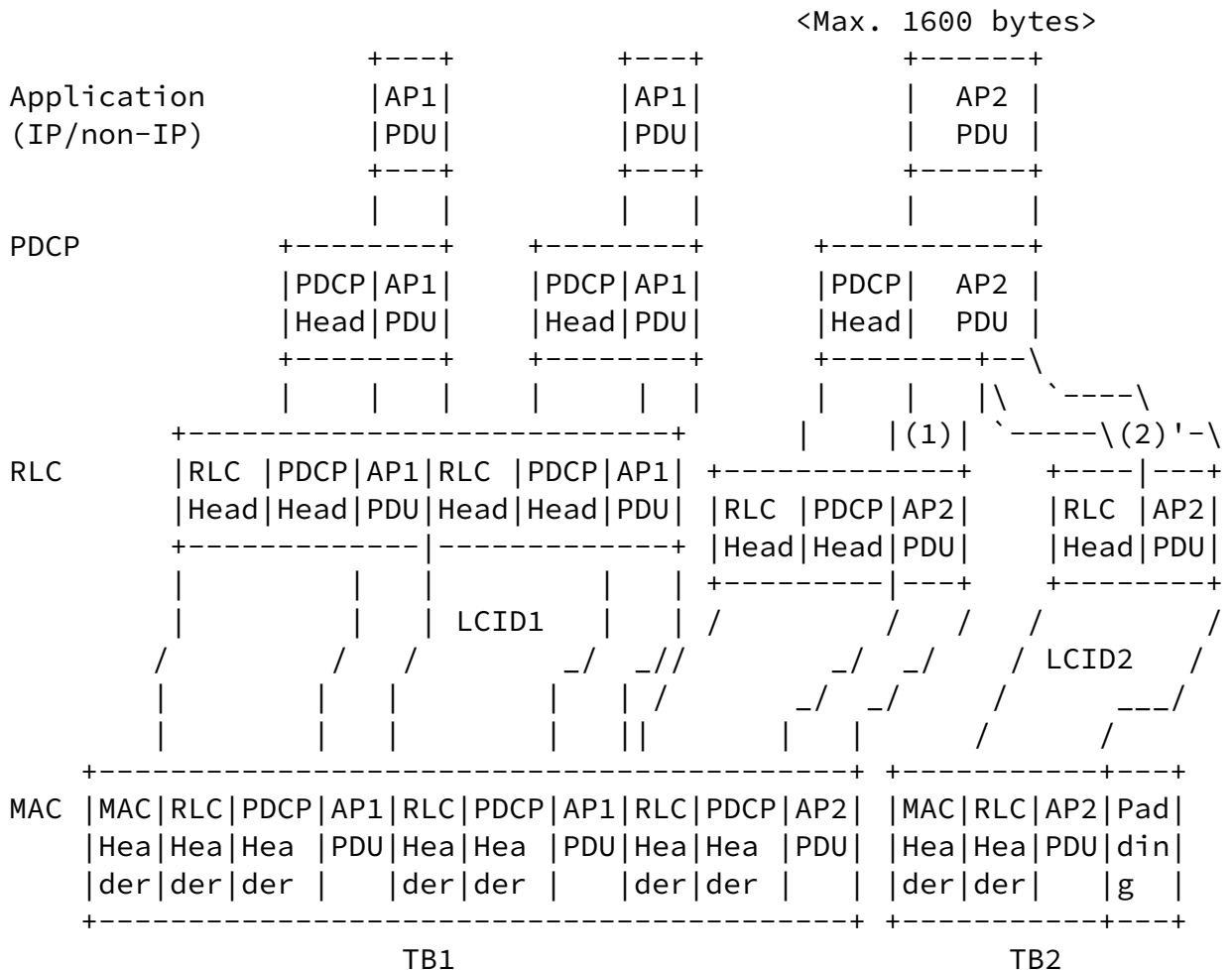


Figure 5: Example of User Plane packet encapsulation for two transport blocks

[10.2.](#) NB-IoT Data over NAS (DoNAS)

The Access Stratum (AS) protocol stack used by DoNAS is somehow particular. Since the security associations are not established yet in the radio network, to reduce the protocol overhead, PDCP (Packet Data Convergence Protocol) is bypassed until AS security is activated. RLC (Radio Link Control protocol) uses by default the AM mode, but depending on the network's features and the terminal, it may change to other modes by the network operator. For example, the transparent mode does not add any header or process the payload to reduce the overhead, but the MTU would be limited by the transport block used to transmit the data, which is a couple of thousand bits maximum. If UM (only Release 15 compatible terminals) is used, the RLC mechanisms of reliability are disabled, and only the reliability provided by the MAC layer by Hybrid Automatic Repeat reQuest (HARQ) is available. In this case, the protocol overhead might be smaller than the AM case because of the lack of status reporting but with the same support for segmentation up to 16000 Bytes. NAS packets are encapsulated within an RRC (Radio Resource Control) TGPP36331 message.

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

Internet-Draft

SCHC NB-IoT

February 2022

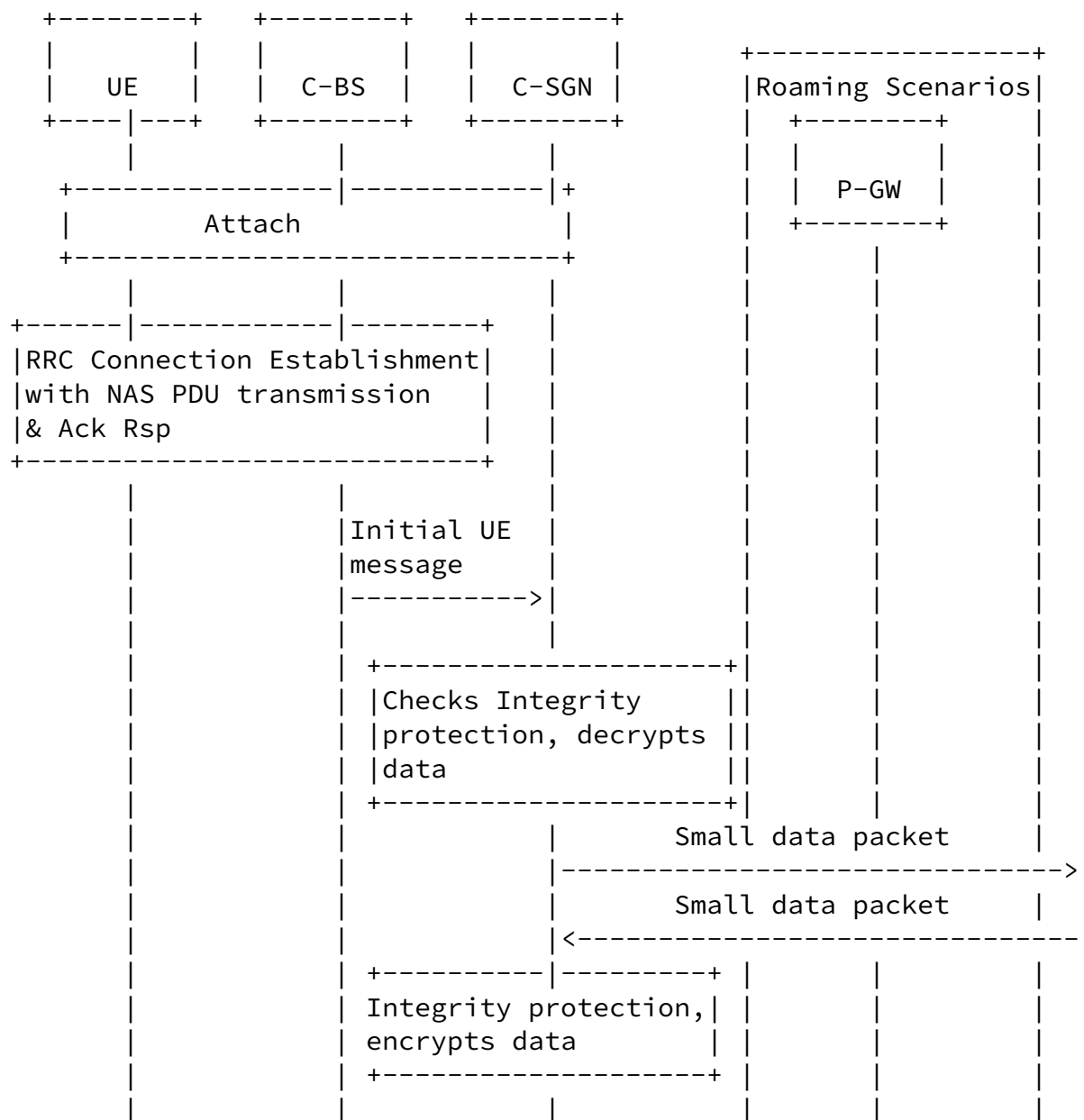


Figure 7: Example of User Plane packet encapsulation for Data over NAS

11. Normative References

- [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>>.
- [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>>.

Authors' Addresses

Edgar Ramos
Ericsson
Hirsalantie 11
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

