lpwan Working Group   A. Pelov
Internet-Draft   Acklio
Intended status: Informational   P. Thubert
Expires: October 30, 2021   Cisco Systems
                                                          A. Minaburo
                                                              Acklio
                                                      April 28, 2021

        LPWAN Static Context Header Compression (SCHC) Architecture
                   draft-pelov-lpwan-architecture-01

Abstract

   This document defines the LPWAN SCHC architecture.

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 October 30, 2021.

Table of Contents

1. Introduction

The IETF LPWAN WG defined the necessary operations to enable IPv6
over selected Low-Power Wide Area Networking (LPWAN) radio
technologies. [rfc8376] presents an overview of those technologies.

The core product of the working group is the Static Context Header
Compression (SCHC) [rfc8724] technology.

SCHC provides an extreme compression capability based on a state that
must match on the compressor and decompressor side. This state if
formed of an ordered set of Compression/Decompression (C/D) rules.
The first rule that matches is used to compress, and is indicated
with the compression residue. Based on the rule identifier (RuleID)
the decompressor can rebuild the original bitstream based on the
residue.

[rfc8724] also provides a Fragmentation/Reassembly (F/R) capability
to cope with a constrained Maximum Transmit Unit (MTU) below the IPv6
minimum link MTU of 1280 bytes (see section 5 of [rfc8200]), which is
typically the case on an LPWAN network.

[rfc8724] was defined to compress IPv6 and UDP; but SCHC really is a
generic compression and fragmentation technology. As such, SCHC is
agnostic to which protocol it compresses and at which layer it is
operated. The C/D peers may be hosted by different entities for
different layers, and the F/R operation may also be performed between
different parties, or different sub-layers in the same stack.

If a protocol or a layer requires additional capabilities, it is
always possible to document more specifically how to use SCHC in that
context, or to specify additional behaviours. For instance,
[I-D.ietf-lpwan-coap-static-context-hc] extends the compression to
CoAP [rfc7252] and OSCORE [rfc8613].

SCHC is also designed to be profiled to adapt to the specific
necessities of the various LPWAN technologies to which it is applied.
Appendix D. "SCHC Parameters" of [rfc8724] lists the information
that an LPWAN technology-specific document must provide to profile
SCHC for that technology. As an example, [rfc9011] provides the
profile for LoRaWAN networks.

In order to deploy SCHC, it is mandatory that the C/D and F/R peers
are provisionned with the exact same set of rules. To be able to
provision end-points from different vendors, a common data model is
needed that expresses the SCHC rules in an interoperable fashion. To
that effect, [I-D.ietf-lpwan-schc-yang-data-model] defines a rule
representation using the YANG [rfc7950] formalism.

Finally, section 3 of [rfc8724] depicts a typical network
architecture for an LPWAN network, simplified from that shown in
[rfc8376]and reproduced in Figure 1.

```
 ()   ()   ()       |
  ()  () () ()     / \         +---------+
() () () () () () /   \======|    ^    |                 +-----------+
 ()  ()   ()     |          | <--|--> |                 |Application|
() () () () () /  \=========|    v    |=============|  Server  |
  ()  ()  ()    /   \         +---------+                 +-----------+
 Dev           RGWs           NGW                          App
```
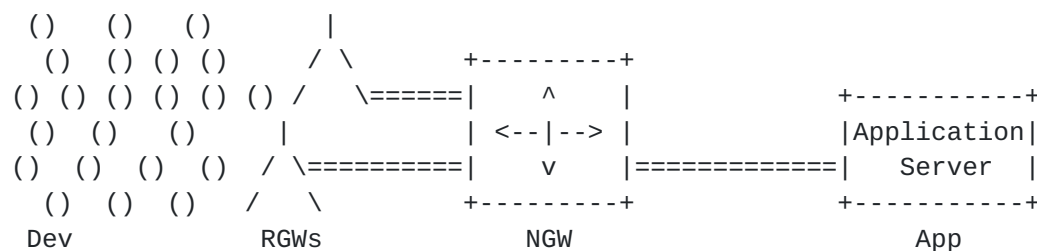
Figure 1: Typical LPWAN Network Architecture

Typically, an LPWAN network topology is star-oriented, which means
that all packets between the same source-destination pair follow the
same path from/to a central point. In that model, highly constrained
Devices (Dev) exchange information with LPWAN Application Servers
(Apps) through a central Network Gateway (NGW), which can be powered
and is typically a lot less constrained than the Devices. Because
devices embed built-in applications, the traffic flows to be
compressed are known in advance and the location of the C/D and F/R
functions (e.g., at the Dev and NGW), and the associated rules, can
be pre provisionned in the network .

Then again, SCHC is very generic and its applicability is not limited
to star-oriented deployments and/or to use cases where applications
are very static and the state can provisionned in advance.
[I-D.thubert-intarea-schc-over-ppp] describes an alternate deployment
where the C/D and/or F/R operations are performed between peers of
equal capabilities over a PPP [rfc2516] connection. SCHC over PPP
illustrates that with SCHC, the protocols that are compressed can be
discovered dynamically and the rules can be fetched on-demand by both

parties from the same Uniform Resource Name (URN) [rfc8141], ensuring
that the peers use the exact same set of rules.

```
+----------+  Wi-Fi /   +----------+               ....
|    IP    | Ethernet |     IP    |            ..          )
|   Host   +-----/------+  Router  +----------(   Internet   )
| SCHC C/D |  Serial    | SCHC C/D |            (          )
+----------+            +----------+               ...
           <-- SCHC -->
              over PPP
```
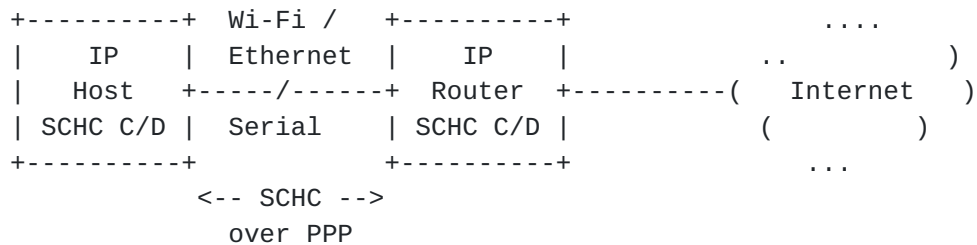
Figure 2: PPP-based SCHC Deployment

This document provides a general architecture for a SCHC deployment,
positioning the required specifications, describing the possible
deployment types, and indicating models whereby the rules can be
distributed and installed to enable reliable and scalable operations.

2. SCHC Operation

As [I-D.ietf-lpwan-coap-static-context-hc] states, the SCHC
compression and fragmentation mechanism can be implemented at
different levels and/or managed by different organizations. For
instance, as represented figure Figure 3, IP compression and
fragmentation may be managed by the network SCHC instance and end-to-
end compression between the device and the application. The former
can itself be split in two instances since encryption hides the field
structure.

```
              (device)                (NGW)                    (App)

            +--------+                                       +--------+
  A S       |  CoAP  |                                       |  CoAP  |
  p C       | inner  |                                       | inner  |
  p H       +--------+                                       +--------+
  . V       |  SCHC  |                                       |  SCHC  |
            | inner  |   cryptographical boundary            | inner  |
 -._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._
  A S       |  CoAP  |                                       |  CoAP  |
  p C       | outer  |                                       | outer  |
  p H       +--------+                                       +--------+
  . C       |  SCHC  |                                       |  SCHC  |
            | outer  |   functional boundary                 | outer  |
 -._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._.-._
  N         .  udp   .                                   .  udp   .
  e         ..........       ..................          ..........
  t         . ipv6  .     .        ipv6      .           . ipv6  .
  w C       ..........       ..................          ..........
  o S       . schc  .     .  schc  .       .                 .       .
  r H       ..........       ..........       .                 .       .
  k C       . lpwan .     . lpwan  .       .                 .       .
            ..........       ..................          ..........
              ((((LPWAN))))               ------   Internet  ------
```
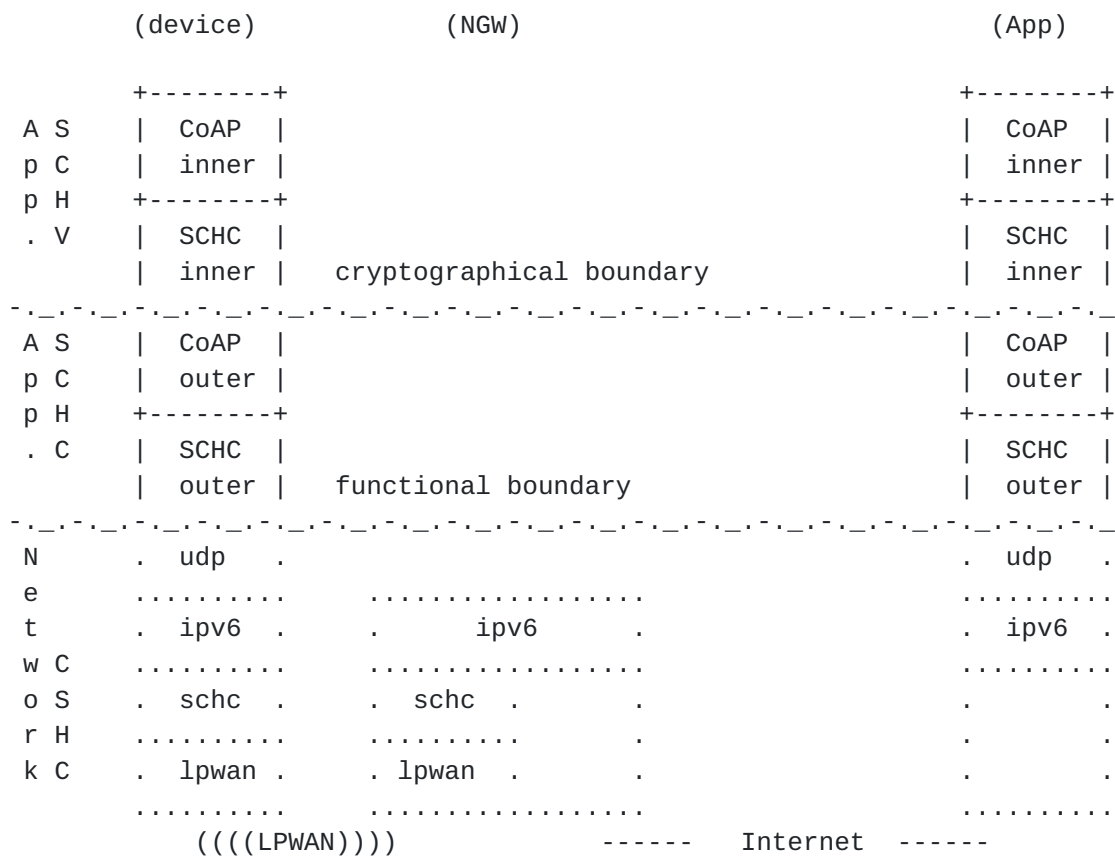
Figure 3: Different SCHC instances in a global system

   This document defines a generic architecture for SCHC that can be
   used at any of these levels. The goal of the architectural document
   is to orchestrate the different protocols and data model defined by
   the LPWAN woeking group to design an operational and interoperable
   framework for allowing IP application over contrained networks.

3. Definitions

4. Global architecture

   As described in [rfc8724] a SCHC service is composed of a Parser,
   analyzing packets and creating a list of fields what will be used to
   match against the compression rules. If a packet matches rules,
   compression can be applied following rules instructions.

   If SCHC compressed packet is too large to be send in a single L2
   frame, fragmentation will apply. The process is similar, device
   rules are checked to find the most appropriate fragmentation rule,
   regarding the SCHC packet size, the link error rate, the reliability
   required by the application, ...

On the other direction, when a packet SCHC arrives, the ruleID is
used to find the rule. Its nature allows to select if it is a
compression or fragmentation rule.

The rule database contains a set of rules specific to a single
device. The [rfc8724] indicates that the SCHC instance reads the
rules to process C/D and F/R, rules are not modified during these
actions.

A SCHC instance, summarized in the Figure 4, implies C/D and F/R
present in both end. The device connected to a constrained network
is in one end and the other end is either located in the core network
or at the application.

In any cases, the rules must be the same in both ends to perform C/D
and F/R.

```
     (device)                                   (core|app)


      (---)                                       (---)
      ( r )                                       ( r )
      (---)                                       (---)
         . read                                      . read
         .                                           .
      +-----+                                     +-----+
  <===| R&D |<=..............................<=| C&F |<===
  ===>| C&F |=>..............................=>| R&D |===>
      +-----+                                     +-----+
```

                   Figure 4: Summarized SCHC elements

To enable rule synchronization between both ends, a common rule
representation must be defined.

5. Data management

[I-D.ietf-lpwan-schc-yang-data-model] defines an YANG data model to
represent the rules. This enables the use of several protocols for
rule management, such as NETCONF, RESTCONF and CORECONF. NETCONF
uses SSH, RESTCONF uses HTTPS, and CORECONF uses CoAP(s) as their
respective transport layer protocols. The data is represented in XML
under NETCONF, in JSON under RESTCONF and in CBOR under CORECONF.

```
                  create
         (-------)  read   +=======+ *
         ( rules )<------->|Rule   |<--|-------->
         (-------)  update |Manager|   NETCONF, RESTCONF or CORECONF
           . read  delete +=======+   request
           .
         +-------+
    <===| R & D |<===
    ===>| C & F |===>
         +-------+
```

                    Figure 5: Summerized SCHC elements

   Rule Manager (RM) is in charge of handling data derived from the YANG
   Data Model and apply changes to the rules database Figure 5.

   The RM is a application using the Internet to exchange information,
   therefore:

   o for the network-level SCHC, the communication does not require
      routing. Each of the end-points having an RM and both RMs can be
      viewed on the same link, therefore wellknown Link Local addresses
      can be used to identify the device and the core RM. L2 security
      MAY be deemed as sufficient, if it provides the necessary level of
      protection.

   o for application-level SCHC, routing is involved and global IP
      addresses SHOULD be used. End-to-end encryption is recommended.

   Management messages can also be carried in the negotiation protocol
   as proposed in [I-D.thubert-intarea-schc-over-ppp]

   The RM traffic may be itself compressed by SCHC, especially if
   CORECONF is used, [I-D.ietf-lpwan-coap-static-context-hc] can be
   used.

6. Acknowledgements

   The authors would like to thank (in alphabetic order):

7. References

7.1. Normative References

   [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>.

7.2. Informative References

   [I-D.ietf-lpwan-coap-static-context-hc]
              Minaburo, A., Toutain, L., and R. Andreasen, "LPWAN Static
              Context Header Compression (SCHC) for CoAP", draft-ietf-
              lpwan-coap-static-context-hc-19 (work in progress), March
              2021.

   [I-D.ietf-lpwan-schc-yang-data-model]
              Minaburo, A. and L. Toutain, "Data Model for Static
              Context Header Compression (SCHC)", draft-ietf-lpwan-schc-
              yang-data-model-04 (work in progress), February 2021.

   [I-D.thubert-intarea-schc-over-ppp]
              Thubert, P., "SCHC over PPP", draft-thubert-intarea-schc-
              over-ppp-03 (work in progress), April 2021.

   [rfc2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D.,
              and R. Wheeler, "A Method for Transmitting PPP Over
              Ethernet (PPPoE)", RFC 2516, DOI 10.17487/RFC2516,
              February 1999, <https://www.rfc-editor.org/info/rfc2516>.

   [rfc7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained
              Application Protocol (CoAP)", RFC 7252,
              DOI 10.17487/RFC7252, June 2014,
              <https://www.rfc-editor.org/info/rfc7252>.

   [rfc7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language",
              RFC 7950, DOI 10.17487/RFC7950, August 2016,
              <https://www.rfc-editor.org/info/rfc7950>.

   [rfc8141] Saint-Andre, P. and J. Klensin, "Uniform Resource Names
              (URNs)", RFC 8141, DOI 10.17487/RFC8141, April 2017,
              <https://www.rfc-editor.org/info/rfc8141>.

   [rfc8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", STD 86, RFC 8200,
              DOI 10.17487/RFC8200, July 2017,
              <https://www.rfc-editor.org/info/rfc8200>.

   [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>.

   [rfc8613]   Selander, G., Mattsson, J., Palombini, F., and L. Seitz,
               "Object Security for Constrained RESTful Environments
               (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019,
               <https://www.rfc-editor.org/info/rfc8613>.

   [rfc9011]   Gimenez, O., Ed. and I. Petrov, Ed., "Static Context
               Header Compression and Fragmentation (SCHC) over LoRaWAN",
               RFC 9011, DOI 10.17487/RFC9011, April 2021,
               <https://www.rfc-editor.org/info/rfc9011>.

Authors' Addresses

   Alexander Pelov
   Acklio
   1137A avenue des Champs Blancs
   35510 Cesson-Sevigne Cedex
   France

   Email: a@ackl.io

   Pascal Thubert
   Cisco Systems
   45 Allee des Ormes - BP1200
   06254 Mougins - Sophia Antipolis
   France

   Email: pthubert@cisco.com

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

   Email: ana@ackl.io