draft-ietf-lpwan-coap-static-context-hc-13

Ana Minaburo

Laurent Toutain

Ricardo Andreasen

Status

- IESG State: AD Evaluation 3 Objection and 7 yes
  - Needs 3 more YES or NO OBJECTION position to pass
- Reviews:
  - IOTDIR: Almost Ready - Minor
  - GENART: Almost Ready – 1 Major, Minor
  - OPSDIR: Ready
  - TSVART: Almost Ready – Minor
  - SECDIR: Serious Issues – Major (partially completed)
- 3 Majors Discussion

Point 1– CoAP Options

- Alexey Melnikov
- Inputs from Francesca Palombini, Benjamin Kaduk
  - Definition of unidirectional/bidirectional
    - Section 5.2 Uri-Host and Uri-Port are unidirectional, contradicts RFC 7252
      - This is only for Max-Age
    - Section 5.4 size1 and size2 are unidirectional only in requests, not accurate with RFC7252 and 7599
  - More options being defined and not specified as:
    - Hop Limit
    - Are they Out of scope or add a discussion about them

Point 1 – CoAP Options

Confusion about Bidirectional / Unidirectional **description**

- SCHC Rule describes each field with some parameters, the direction is one (UP, DW, BI)
- A field may appear several times in a Rule depending on the direction values
- So a FID can be described as UP or DW and BI with different TV/MO/CDA
  - IF a field has the same TV/MO/CDA in both direction a BI description is used

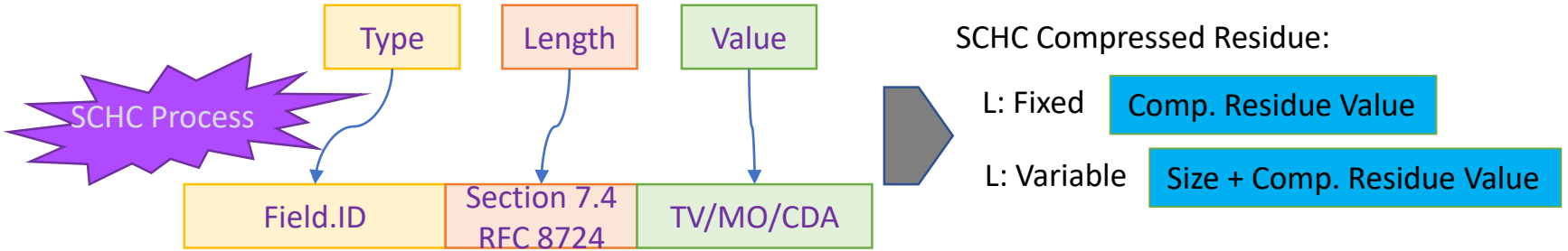
  But
  - IF a field is present in both directions but has different values in each direction then two description UP and DW are used
  - IF a field is present in only one direction so one description is used UP or DW

SCHC does not change the nature of a bidirectional Option
But describe a Bidirectional Option in two Unidirectional Values

Point 1 – CoAP Options

The Draft does not describe all the Options, What will happen with new options?

- Add description in section 5 for the generic TLV compression (New)
- Semantics definition for TLV compression

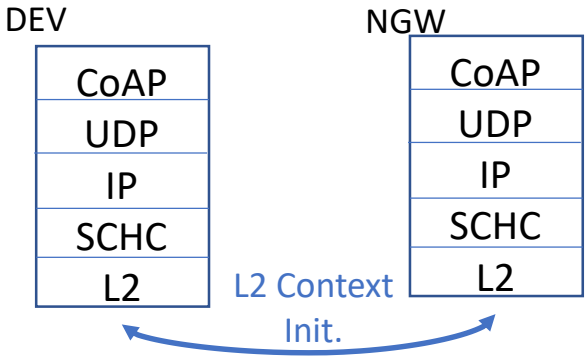


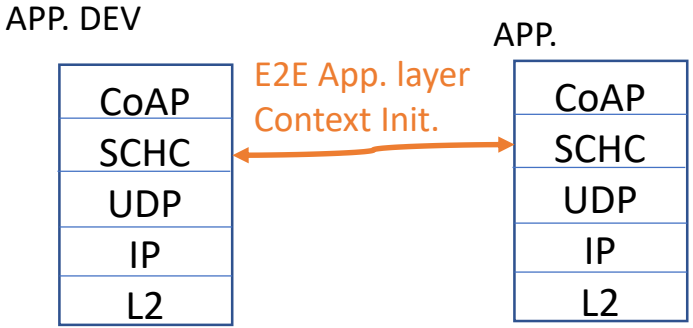
Point 2 – Context Initialization - Architecture

- Magnus Westerlund
  - Perspective of context establishment between APP – APP
  - Different from a L2 context establishment between the DEV and the NGW

Point 2 – Context Initialization - Architecture

- Context Initialization is done between Device and NGW in L2
- BUT when doing compression of CoAP layer, the compression is done in the Application layer only. E2E context initialization has to be negotiated differently.
- => Important point for the Architecture of SCHC
- => Out of the scope but a NOTE has been introduced in the Section 2.





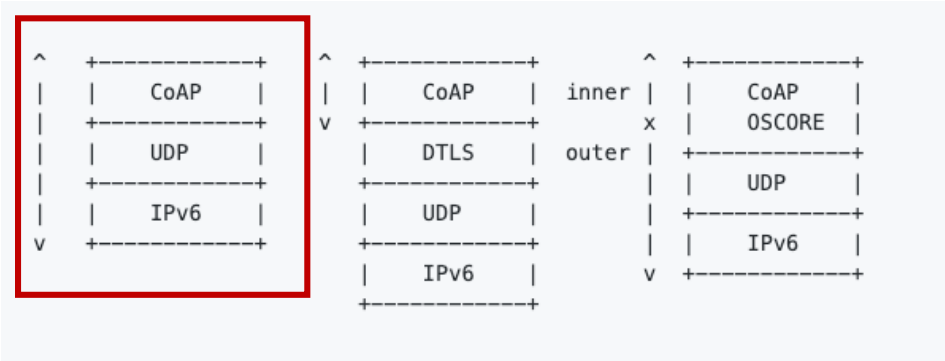
Point 3 – Security Section

- SECDIR review (Paul Wouters)
- Review Result: Serious Issues
  - Suresh ask to see this point quickly

- Agree with GEN-ART security inputs
- Coordinate both documents to determine where, how and which Security Considerations are relevant
- Worried multiple layers doing compression. Can this lead to security issues? If not, why not?
- Where is it says that compression need to be checked for bogus instructions?
  - How are these prevented?
  - Think of the ever-decompressing zip file hacks of the past
  - How are these DoS attacks prevented?

Point 3 – Security Section

- Benjamin Kaduk (answering Paul Wouters)
  - Both documents needs coordination for the security section
  - Many expected use case when: CoAP is not guaranteed to be used over a physical medium integrated security technologies
    - The case where CoAP is over UDP/IP without any security protocol section 2 draft CoAP



Point 3 – Security Section

- New Text for Section 9.

The **Security Considerations** of SCHC header compression **RFC8724 are valid** for SCHC CoAP header compression.

When CoAP **uses OSCORE** in the communication, **the security considerations** defined in **RFC8613 does not change** when SCHC header compression is applied.

The definition of **SCHC over CoAP** header fields permits the compression of header information only. The SCHC header compression itself **does not increase or reduce the level of security** in the communication.

In the case when the communication does **not use any security** protocol as OSCORE, DTLS, or other. **It is highly necessary to use a layer two security.**

A corrupted header compressor could cause the header decompressor to reconstitute packets that do not match the original ones, but still have valid headers and possibly also correct transport checksums. SCHC header compression scheme uses an **Integrity Check** to verify the reconstructed headers, which reduces the probability of producing decompressed headers not matching the original header without being noticed. **End-to-End Authentication and Integrity mechanisms may detect** such corruption.

DoS attacks are possible if an intruder can introduce a compressed SCHC corrupted packet onto the link and **cause a compression efficiency reduction**. However, an intruder having the ability to add corrupted packets at the link layer raises **additional security issues than those related to the use of header compression.**

SCHC compression **returns variable-length Residues** for some CoAP fields. In the compressed header, the length sent is not the original header field length but the length of the Residue. So if a corrupted packet comes to the decompressor with a longer or shorter length than the one in the original header, **SCHC decompression will detect an error and drops the packet**.

Point 3 – Security Section

- No Input from the ML
- Any input is welcome

Next steps

- Answer to all the reviewers
- Submit new version with all inputs

- Thank you
- Questions?

- Keep Safe!